

Moral and Legal Foundations of Privacy

January 31, 2023



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

1

Privacy: What Is It?



“Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.”

- Judith Jarvis Thomson, *The Right to Privacy*

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

2



Privacy: What Is It?

- We must distinguish between two interrelated concepts:
 - The concept of privacy – “what is privacy?”
 - The right of privacy – “what does the law protect/prohibit?”
- “The law does not determine what privacy is, but only what situations of privacy will be afforded legal protection.” - Hyman Gross



I. Philosophical Perspectives on Privacy



Wasserstrom – Privacy: Some Arguments and Assumptions

What Is Privacy, and What Control Does One Have over It?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

5

Wasserstrom – Privacy: Some Arguments and Assumptions



Discusses what privacy is by four scenarios:

1. You are sitting in a chair resting with ideas, emotions, and sensations running through your mind.
2. You are in a closed telephone booth talking to a travel agent (or at home having dinner with your spouse).
3. You are in your bedroom with your spouse.
4. You are considering hiring a research assistant, and you can get a printout with age, marital status, arrest record, grades, income, and what they have done.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

6

Wasserstrom – Privacy: Some Arguments and Assumptions



- Scenario #1 – Your thoughts: This involves facts that only you can know unless you take the step of telling someone or providing access to your body (mind reading, etc.).
- Scenario #2 – Phone Booth / Dinner: Less in your control than thoughts, as the agent/wife can pass on what you said.
- Scenario #3 – With Spouse in Bed: Similar to the phone booth or dinner, except that you have a reasonable expectation that the information will not be passed on.

Wasserstrom – Privacy: Some Arguments and Assumptions



- Why are “thoughts” so innately private?
 - They are intimate and unfiltered – often uncontrollable.
 - We would not want to be accountable for our thoughts.
 - Our thoughts and feelings are what make us a person and part of being a person is having control over our internal and unique feelings and thoughts.
- Helps explain 5th Amendment (right against self-incrimination): you cannot be required to disclose your thoughts.
 - But the government can take a blood sample, because it’s not the same as a thought you possess.

Wasserstrom – Privacy: Some Arguments and Assumptions



- California Department Store Example: Police were drilling holes in the bathroom ceiling to enable watching to catch illegal activity.
- Found to be illegal (unlawful search and seizure, which we will learn in the 4th Amendment portion of class)
 - Wasserstrom asserts that it was also partially because of the violation of privacy of all the persons observed, not just those arrested.

Wasserstrom – Privacy: Some Arguments and Assumptions



- More than thoughts are private: “doing something in private” and “doing a private kind of thing”.
- Telling people different things in private (or not telling them) is how we gauge many relationships.
- “Private kinds of things” are done only when we reasonably believe we are in private.
- Even if you know you are going to be observed, there is an effect – you may act differently as a result.

Wasserstrom – Privacy: Some Arguments and Assumptions



- The “Data Bank” example:
 - All the information about you is somehow extractable.
 - Article is from 1978 but sounds like Wasserstrom could see the future; that’s where we are now.
- You could make some qualitative analysis about who I am.
- You can also roughly figure out where I was and what I was doing.
- Concerns are raised about accuracy, amount, aggregation.

Wasserstrom – Privacy: Some Arguments and Assumptions



- What are the consequences on attitudes toward privacy in society?
 - What we think is private will change if we’re used to giving up such information and having it mined.
 - May alter the ways we consider relationships with one another.
 - Both of these are arguably happening now, especially for persons that may have a lower expectation of privacy. Expectations of privacy have changed.
 - Downloads, Terms of Use, Privacy Policies, Tweets.

Wasserstrom – Privacy: Some Arguments and Assumptions



- Is there another approach that will tie these issues together? Wasserstrom says yes.
- Calls is the “perspective of counterculture.”
 - We act as different people in public and private (the “Real Person” argument).
 - PoC confronts the thought that there are facts we keep private because they would be embarrassing or shame-worthy.
 - If these thoughts were known, and it turned out we all had them, they would cease to be bad.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

13

Wasserstrom – Privacy: Some Arguments and Assumptions



- He says the same goes for acts: We are conditioned by culture to think that sex must be private.
- But would it be just as enjoyable in public if the culture were different?
 - Does a good dinner taste better at home or in a restaurant?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

14

Wasserstrom – Privacy: Some Arguments and Assumptions



- What would be gained or lost from such a change in the culture?
 - Would intimacy either as friendships or relationships be weakened or less likely since they are based in part on sharing intimate things?
 - Would day to day relationships get vastly more complicated if we had such openness with everyone about everything?

Thomson – The Right to Privacy

The Reductionist View of Privacy



Thomson – The Right to Privacy

- Like Wasserstrom, Thomson uses several examples to discuss the bounds of privacy:
 1. Husband and wife having a fight heard from the street and windows are open.
 2. Husband and wife having a quiet fight and someone uses an amplifier to hear.
 3. Same as #1 but hard of hearing person walks by and turns up his hearing aid to listen.
 4. Two people talking in the park, man creeps around the bushes to hear.



Thomson – The Right to Privacy

- Another example: A man has a pornographic picture that he keeps in his wall safe.
- Owning a picture – does it include the “negative” right to prevent others from seeing it? Or that it shall not be looked at?
- Sometimes you have a right that can be waived – you accidentally leave out the picture.
- To what extent does the man have to protect the picture? Encase his house in platinum?



Thomson – The Right to Privacy

- Why this discussion? If we have such rights over property, we therefore must have such rights over ourselves.
- Those rights are relative based on circumstances. Examples on pp. 303-304.
- Thus, much like the picture and property, privacy is a “cluster of rights,” and in fact overlaps with it and the “rights over the person.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

19



Thomson – The Right to Privacy

- No right that a fact shall not be known; rather, that certain steps shall not be taken, and certain uses shall not be made of such facts.
- Using an x-ray to see someone is improper steps to gain information.
- The information must be personal.
- Posits that you may not have a violation of privacy without some other violation:
 - Compare sending a letter with torture.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

20

Thomson – The Right to Privacy



- If you gain information with the caveat that you are not to spread it, and you do, that is a violation of privacy (if it was personal information), because you also have a violation of confidentiality.
- I publicize that you have a pornographic picture in your safe at home: may be a violation of privacy IF you also see a violation of the right to be free of distress.
 - BUT, Thomson says this is trumped by the right of free press.
- Thus, right to privacy is derivative – it always is associated with another right (pages 312-314).

Rachels – Why Privacy Is Important

A Response to Thomson: Privacy as a Condition of Relationships

Rachels – Why Privacy Is Important



- Response to Thomson's "cluster of rights."
- Starts with a basic definition of privacy as "a characterization of the special interest we have in being able to be free from certain kinds of intrusions."

Rachels – Why Privacy Is Important



- Different interests:
 - Competitive interests: Bobby Fisher's chess analysis
 - Embarrassment: "End of the Road" story (spying)
 - Medical Records
 - Credit Applications
- But, these do not help with a complete understanding of privacy.
 - They are unique.
 - Are often objectionable on other non-privacy grounds.

Rachels – Why Privacy Is Important



- We need to understand the “something important” about privacy that makes something “someone’s business” or “none of your business.”
- Takes issue with the “Real Person” argument (Wasserstrom), i.e. that beneath the different ways a person interacts with different people is a real person.

Rachels – Why Privacy Is Important



- Rather, he posits that we simply have different understandings of different situations; none of them is necessarily “dishonest” or not real (but they can be, of course).
- These can change from person to person, and from society to society.
- Group therapy – you cease to think of each other as strangers, but rather as fellow members of the group.
- Things that impede on the ability to have the relationships we want in the way we want is often considered objectionable, and why we value privacy.

Rachels – Why Privacy Is Important



- Example: Close friends joined by a casual acquaintance necessarily changes the dynamic.
 - What if the close friends were never alone? They would either need to share confidences in violation of how they want to be around the casual acquaintance, or not share close information, meaning that they could no longer be close friends.
- Thus, if we cannot control who has access to us, we cannot control our relationships, impeding privacy.

Rachels – Why Privacy Is Important



- What about facts that are “simply nobody else’s business?”
 - Depends on the relationship – a doctor gets different access than an employer.
 - Such relationships are generally voluntary.
- However, once entered, we cannot expect the same degree of privacy as before.
 - “How much money is in your bank account” is not private to your banker, creditor, or spouse. But as to others, it may well be.



Rachels – Why Privacy Is Important

- Takes issue with Thomson's attempt to say privacy is a "cluster" of rights that intersects with the right over the person, and the cluster of rights over property.
- Rachels says that, for example, the right not to have various parts of your body looked at is not analogous to property rights, and such subject to societal norms. A question of degree, and therefore different from property.



Rachels – Why Privacy Is Important

- Rachels also rebuts the "very personal gossip" argument – Thomson argued that if the information was obtained without violating your rights and disclosed without violating a confidence, there is no violation of a right to privacy in disclosing it.

Rachels – Why Privacy Is Important



- Rachels thinks his understanding of privacy means there may be a violation in such a case:
 - What if you were overheard telling a friend the intimate information, and that other person discloses it?
 - There was not also a right over property or the person, but it would still be a violation of the right to privacy because of our right to control who has access to us.
 - Privacy is a protection here because it has a “different point” than the other rights.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

31

Three Viewpoints So Far...



- Wasserstrom: Privacy hides who we are as “real people”
- Thomson: Privacy is derivative of your pre-existing “Cluster of Rights”
- Rachels: Privacy is a condition of relationships

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

32



Reiman – Privacy, Intimacy, and Personhood

A Response to Thomson and Rachels:
Privacy as a Condition of Personhood

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

33

Reiman – Privacy, Intimacy, and Personhood



- A follow-on to Thomson and Rachels.
- Also disagrees with Thomson, but thinks Rachels does so for the wrong reason.
- Says Thomson's premise that privacy is a derivative right is a non sequitur.
 - Assuming that privacy rights overlap with property and personal rights does not prove that privacy is derivative from these rights.
 - In fact, this assumption is consistent with the opposite conclusion: that all property and personal rights are derivative from a privacy right.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

34

Reiman – Privacy, Intimacy, and Personhood



- Even if you agreed with Thomson's hypothesis, it does not follow that you do not need to or want to find out what is common to the cluster of rights in the right to privacy.
- Finding out what is common may help resolve difficult moral conflicts.
- Reiman says there is something unique, and promises a conclusion. But first, he rebuts Rachels.

Reiman – Privacy, Intimacy, and Personhood



- According to Reiman, Rachels is wrong in his analysis starting with his basic definition of privacy as "a characterization of the special interest we have in being able to be free from certain kinds of intrusions."
- Reiman says this definition is circular: saying privacy is the right to be free from certain intrusions is no more than saying that "rights to privacy protect our special interest in privacy."



Reiman – Privacy, Intimacy, and Personhood

- Reiman also takes issue with Rachels' conclusion that privacy, and thus our selection of what and whom to share certain things, allows us to create and maintain our relationships with other people.
- This has a logical end: if you give full access of everything to everybody, you can't have any friendships because there is no special sharing with anyone not shared with everyone.
 - Is there any truth to this logic in the current digital age?
- Reiman finds this problematic; the value of intimacy then lies not in what you have, but what others do not have.



Reiman – Privacy, Intimacy, and Personhood

- Rachels also misses the context of the sharing, which to Reiman is more important than the content shared.
- You share information with a psychoanalyst that you wouldn't share with a friend, but that does not make the analyst relationship more intimate.
- If you share the information with a friend, it means something more because of the "context of caring." You care about each other.
- Rachels also makes the right to privacy derivative like Thomson, but derivative from social relationships.

Reiman – Privacy, Intimacy, and Personhood



- Reiman thinks Benn comes closer to the right answer: privacy is the principle of respect for persons as choosers of what and to whom they share.
- But Benn is too broad. It would give us a right not to have people glance at us walking down the street or stare us in the face if we didn't "choose" for them to do so.

Reiman – Privacy, Intimacy, and Personhood



- So what is the fundamental interest?
 - "Privacy is a social ritual by means of which an individual's moral title to his existence is conferred."
- Privacy is what defines us as persons:
 - "Privacy is necessary to the creation of selves out of human beings, since a self is at least in part a human being who regards his existence—his thoughts, his body, his actions—as his own."

Reiman – Privacy, Intimacy, and Personhood



- “The right to privacy, then, protects the individual’s interest in becoming, being, and remaining a person. It is thus a right which all human individuals possess.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

41

Parent – Privacy, Morality, and the Law

The Informational View of Privacy

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

42



Parent – Privacy, Morality, and the Law

- “Privacy is the condition of not having undocumented personal knowledge about one possessed by others.” W.A. Parent, *Privacy, Morality, and the Law* (1983).
 - Drinking? Drug Use? Height? Income?
- “Personal Information”: “facts which most persons in a given society choose not to reveal about themselves . . . or facts about which a person is acutely sensitive and which he therefore does not choose to reveal about himself, even though most people don’t care if these same facts are widely known about themselves.”
- Other definitions wrong...pages 271-274

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

43



Parent – Privacy, Morality, and the Law

- Is information that fits the definition, but that is obtained legitimately still private?
- Parent’s example: Reading old newspapers, you find Bob’s name in a story about child prodigies who failed to succeed as adults. Bob has become a gambler and alcoholic.
 - Have you invaded Bob’s privacy?
 - What if you then publish that information in a magazine?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

44

Parent – Privacy, Morality, and the Law



- Parent says no: it may harm Bob's reputation, but his privacy – as defined by Parent – is not changed.
 - Does it matter if Bob told you in confidence?
 - Does it matter if Bob's friend told you about Bob?

Parent – Privacy, Morality, and the Law



- His example:
 - A person who voluntarily divulges all sorts of intimate, personal information about himself to a friend.
 - He says that while that person exercises control over the personal information, it has ceased to be private.
 - The other definitions, he argues, do not allow for this situation, as they would argue the information could still be private.

Parent – Privacy, Morality, and the Law



- Why? Because these theories mistake privacy as a part of liberty, which it is not.
- Thus, he argues, laws that prohibit actions (contraception, abortion, or anything else), do not impact privacy in what a person chooses to do, but rather that person's liberty.

Inness – Privacy, Intimacy, and Isolation

The Decisional View of Privacy

Inness – Privacy, Intimacy, and Isolation



- What is the content of privacy? Intimacy of information defines it.
- Three common considerations:
 - Information-based: the ability to regulate information about ourselves, but can lose privacy w/o losing information.
 - Access-based: the ability to regulate access to ourselves, but doesn't mean private information lost.
 - Decision-based: the ability to regulate decisions about our actions, but not all such decisions are privacy-related.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

49

Inness – Privacy, Intimacy, and Isolation



- Why is the informational definition insufficient?
 - Simply being “information” is not a sufficient condition to be within the scope of privacy.
 - The “intimacy” of the information is what matters.
 - Would “secrecy” be a better consideration?
 - Not inherently positive, covers “non-intimate” information.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

50

Inness – Privacy, Intimacy, and Isolation



- “Information Based” problems, cont’d:
 - Do not require information loss to have loss of privacy.
 - Peeping Tom example: you have not lost information, but you have lost your privacy.

Inness – Privacy, Intimacy, and Isolation



- Access-based privacy:
 - “The state of an agent have control over access to herself.”
 - Does this address the problems with “information-based” privacy?
 - Addresses the Peeping Tom problem.
 - Learning “information” can be seen as the result of access.
 - However, not all access impacts privacy;
 - Non-intimate access: glance in public, etc.

Inness – Privacy, Intimacy, and Isolation



- Constitutional issues seem to go further – about our right to decide to take actions, rather than access to information.
- Does this mean “decisional” privacy goes beyond “access” privacy?
- “Liberty of action” is better name than “decisional”?

Inness – Privacy, Intimacy, and Isolation



- Three problems:
 - 1. “Decisional privacy” involves liberties with different features.
 - 2. Does not explain why we confuse them.
 - 3. Undermines “access-based” privacy.
- So how do we reconcile them?
 - Define them both by way of control over intimate decisions.

Inness – Privacy, Intimacy, and Isolation



- Inness' position is that you cannot focus on any one of these because privacy involves all three areas.
- Rather, she asserts that "the common denominator of intimacy" governs.
- Thus "privacy's content covers intimate information, access, and decisions."

Inness – Privacy, Intimacy, and Isolation



- Her conclusion:
 - "Privacy can be defined as the state of an agent possessing control over a realm of intimacy, which includes her decisions about intimate informational access, intimate access, and intimate actions."

Moral and Legal Foundations of Privacy

February 7, 2023



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

1

Recap of Last Week



- Six philosophical articles that attempt to define “privacy”
 1. Wasserstrom
 - Introduction to concepts of privacy and how society can affect the definition of privacy
 - “Perspective of counterculture”
 2. Thomson – the “reductionist view” of privacy
 3. Rachels – privacy is a condition of our relationships
 4. Reiman – privacy is a condition of personhood
 5. Parent – the “informational view” of privacy
 6. Inness – privacy requires “intimacy”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

2

II. The Emergence of a Legal Right to Privacy



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

3

Warren/Brandeis: The Right to Privacy



A Legal Definition of Privacy:
The “Right To Be Let Alone”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

4

Warren/Brandeis – The Right to Privacy

- Traces how the law has gone from remedy only for physical interference with life and property, and has broadened to now (in 1890):
 - the right to life includes to enjoy life;
 - “the right to be let alone,”
 - right to liberty, and
 - property included tangible and intangible.
- They say the time has come for the next step: a defined and protected “right to be let alone.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



5

Warren/Brandeis – The Right to Privacy

- Why? “The press is overstepping in every direction the obvious bounds of propriety and of decency.”
- Yet, the intensity and complexity of life requires that solitude and privacy have become more essential for retreat.
- Gossip belittles and perverts.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

6

Warren/Brandeis – The Right to Privacy

- Goal of the article:
 - First, does existing law afford a principle which can properly be invoke to protect the privacy of the individual; and
 - Second, if it does, what is the nature and extent of such protection?
- Then-current slander/defamation law was not enough. It requires injury to reputation. Thus, material damage rather than “spiritual” damage.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



7

Warren/Brandeis – The Right to Privacy

- No current law for injury of feelings other than to alter damages for some other harm. It does not stand alone.
- Common law secures the right to what extent a person’s thoughts, sentiments and emotions shall be communicated. Even if expressed, one can generally limit the publicity of them (think IP: patent, copyright).
- One only loses that right when the information is published publicly.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

8

Warren/Brandeis – The Right to Privacy



- The right to prevent publication of manuscripts or works of art differs from copyright or other traditional property.
- The value is in “the peace of mind or the relief afforded by the ability to prevent any publication of it at all.”
- The content or uniqueness of the information does not matter, and the prohibition is not just limited to copying, but also to summarizing, conveying, etc.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

9

Warren/Brandeis – The Right to Privacy



- Thus, the protection of thoughts, etc., is the more general “right of the individual to be left alone.”
- It is like other exclusionary rights – the right not to be assaulted or beaten, not to be imprisoned, maliciously prosecuted, or defamed, as each of these are rights possessed by the person that the law protects.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

10

Warren/Brandeis – The Right to Privacy



- This right “to be let alone” would protect against the press or new technological advances.
- It is not limited to things reduced to writing – it protects the thought, emotion, or feeling.
- Nor does the amount of effort required to create the thought matter; it is impracticable.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

11

Warren/Brandeis – The Right to Privacy



- The authors go through a number of examples, but in each there was an actual contract that was breached in some way.
- The authors argue that the premise in those decisions – of implying a trust – is a declaration that public morality requires such action.
- The authors believe that the courts can hardly stop there (at contract actions).

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

12

Warren/Brandeis – The Right to Privacy



- Press and modern devices allow for perpetration of similar wrongs without any participation by the injured party (unlike a contract), and thus the protection must have a broader basis.
- For example, taking a picture surreptitiously should not be allowed simply because the target did not know.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

13

Warren/Brandeis – The Right to Privacy



What about limitations on the right to privacy?

- The authors identify 6 limits:
 1. The right to privacy does not prohibit any publication of matter which is of public or general interest.
 - Are you a public person or not?
 - Matters include private life, habits, acts, and relations of an individual and have no relation to his public office or capacity.
 - Though there are some things that could be private regardless.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

14

Warren/Brandeis – The Right to Privacy



2. The right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

15

Warren/Brandeis – The Right to Privacy



3. The law would probably not grant any redress for the invasion of privacy by oral publication in the absence of special damage.
 - This is because the injury resulting from such oral communications is so small that, in the interest of free speech, should not be actionable.
4. The right to privacy ceases upon the publication of the facts by the individual, or with his consent.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

16

Warren/Brandeis – The Right to Privacy

- 5. The truth of the matter published does not afford a defense.
 - This is because redress would not be sought for injury to the reputation of the person. Slander and libel can address that situation. The right to privacy "implies the right not merely to prevent inaccurate portrayal of private life, but to prevent its being depicted at all."
- 6. The absence of "malice" by the publisher does not afford a defense. Same logic.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



17

Warren/Brandeis – The Right to Privacy

- What about remedies for a violation?
 1. An action of tort for damages in all cases.
 - "Compensation for injury to feelings."
 - Is that too speculative? How do you calculate it?
 2. Injunctions, "in perhaps a very limited class of cases."
 - But wouldn't this be better since the harm is effectively irreparable – you can't un-ring the bell.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

18

Spears – The Case That Started It All: Roberson v. Rochester Folding Box Co.

One Court Rejects the "Right to Be Let Alone" as Natural Law

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



19

Roberson v. Rochester Folding Box Co.

- Defendant Franklin Mills Co. made 25 thousand lithographic prints of a woman without her consent and used it in advertising.
- Plaintiff (the woman) was ridiculed by acquaintances and others.
- She alleged damages of \$15,000 from stress, etc.
- She also sought an injunction against further use.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

20

Roberson v. Rochester Folding Box Co.



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

21

Roberson v. Rochester Folding Box Co.

- Plaintiff did not allege libel/slander; the likeness of her in the advertisement was actually very good.
- The lower court found that while there was no precedent, there is a valid cause of action for invasion of the "right to privacy."
- Appellate court calls it the "right to be let alone."
- The court is concerned about opening a Pandora's Box.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

22

Roberson v. Rochester Folding Box Co.



- The Court decides it needs to consider the cases cited in the Brandeis/Warren article to understand whether they truly embodied what Brandeis/Warren argue, or are just property cases and not part of a right to privacy.
- Finds that many of the cases were based on a breach of contract, trust or violation of property right, and NOT based on the feelings of the individual involved.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

23

Roberson v. Rochester Folding Box Co.

- *Dockrell v. Dougall* (1898): True but unauthorized statement by a doctor about a product used in advertising.
 - The Court said this was not actionable unless there was injury to reputation or property.
- *Chapman v. Telegraph Co.*: The law does not provide redress for injury to feelings due to mere negligence.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

24

Roberson v. Rochester Folding Box Co.



- *Corliss v. E.W. Walker*: Court stated that “a private individual has the right to be protected from the publication of his portrait in any way,” but found Mr. Corliss to be a public figure.
- *Roberson* Court takes issue with the *Corliss* decision: “The line between public and private characters cannot possibly be drawn.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

25

Roberson v. Rochester Folding Box Co.



- As a result, the Court felt that absent legislation, there was no basis for the Court to determine or enforce a right to privacy.
- *Atkinson v. Dougherty*: use of the likeness of a deceased person; family sued to enjoin. The Court found for the defendant, stating that while what was done was repugnant “The law does not remedy all evils.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

26

Roberson v. Rochester Folding Box Co.



- Not surprisingly, the Court finds no cause of action.
- BUT refers to Penal Code section 242, relating to “malicious publication by picture, effigy, or sign, which exposes a person to contempt, ridicule or obloquy, is a libel, and it would constitute such at common law.”
- So, doesn’t the Plaintiff have a case?
 - The Court allowed the Plaintiff to amend.
- The Court also noted that the legislature could act and change the law

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

27

Roberson v. Rochester Folding Box Co.



- The NY State Legislature subsequently amended the law following public uproar about the decision.
- Section 50 prohibits the use of a living person’s “name, portrait or picture” for commercial purposes without the person’s consent.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

28

Kent: Pavesich, Property and Privacy

(Pavesich v. New England Life Insurance Co.)

A Different Court Affirms the Right to Privacy as a Natural Right

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

29

Pavesich v. New England Life Insurance Co.

- Rebuttal to the *Roberson* case.

- Atlanta Journal-Constitution published likeness of Plaintiff as part of an advertisement run by the insurance company. He was portrayed in a positive manner.
- He never had a policy or made statements attributed to him.
- Lower court sustained dismissal for lack of claim.
- Georgia Supreme Court reversed.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

30



THE CONSTITUTION, ATLANTA, GA., SUNDAY, NOVEMBER 15, 1895.
THESE TWO PICTURES TELL THEIR OWN STORY.
"In my healthy and productive period of life I bought insurance in the New England Mutual Life Insurance Co. of Boston, Mass., and today my family is protected and I am drawing an annual dividend on my paid-up policies."

THOMAS B. LUMPKIN, General Agent,
1008-1009-1010 EMPIRE BUILDING.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

31

Pavesich v. New England Life Insurance Co.

- The absence for a long period of time of a precedent for an asserted right is not conclusive evidence that the right does not exist.
- Where the case is new in principle the courts cannot give a remedy, but, where the case is new only in instance, it is the duty of the courts to give relief by the application of recognized principles.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

32

Pavesich v. New England Life Insurance Co.

- A right of privacy is derived from “natural law.”
 - Goes to Roman times. See page 4 of the case.
- The right of privacy is embraced within the absolute rights of “personal security” and “personal liberty.”
 - Explained on page 5 of the case.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

33

Pavesich v. New England Life Insurance Co.

- Response to *Roberson*: Says that the cases that the *Roberson* court focused on were not the right sources. Others show a right to privacy.
- Liberty of speech and of the press, when exercised within the bounds of the constitutional guaranties, are limitations upon the exercise of the right of privacy.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

34

Pavesich v. New England Life Insurance Co.

- The publication of one's picture, without his consent, for commercial purpose, is in no sense an exercise of the liberty of speech or of the press, within the meaning of those terms as used in the Constitution.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

35

Prosser – Privacy

How Do We Define a Legal Violation of a Right to Privacy?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

36

Prosser – Privacy

- The article Attempts to synthesize the various privacy decisions.
- It finds “four distinct kinds of invasion of four different interests of the plaintiff which are tied together by a common name, but otherwise have almost nothing in common....” Page 107.
- Basically a rebuttal of the Brandeis/Warren article’s amorphous definition of privacy.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

37

Prosser – Privacy

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

38

Prosser – Privacy

- Intrusion:
 - Includes both physical and other types of intrusion (eavesdropping, etc.).
 - BUT the intrusion must be something which would be offensive or objectionable to a reasonable man.
 - “It is clear also that the thing into which there is prying or intrusion must be, and be entitled to be, private.”
Page 108.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

39

Prosser – Privacy

- Public Disclosure of Private Facts:
 - First, the disclosure of the private facts must be a public disclosure, and not a private one.
 - Second, the facts disclosed to the public must be private facts, and not public ones.
 - Being seen in public is not private (but adding commentary can be a separate violation).
 - What about the lapse of time? The *Melvin* case (ex-prostitute who turned good, later movie about her previous life).
 - Maybe there are limits?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

40

Prosser – Privacy

- Public Disclosure of Private Facts (cont'd):
 - Third, the matter made public must be one which would be offensive and objectionable to a reasonable man of ordinary sensibilities.
 - *Sidis* case regarding child prodigy (newspaper follow-up, led to the bookkeeper's early death).
 - Prosser suggests a "mores" test given the differing results in *Melvin* and *Sidis*.
- Claims that this is different from intrusion, because reputation is the interest.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

41

Prosser – Privacy

- False Light in the Public Eye
 - Need not be defamatory.
 - But must be objectionable to the ordinary reasonable man.
 - Prosser again suggests "mores."
 - The interest is also reputation, but differs from public disclosure because one deals with truth and the other falsity.
 - Concerns regarding whether this overwhelms defamation.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

42

Prosser – Privacy

- Appropriation
 - One makes use of another's name to pirate the other's identity for some advantage of his own
 - Impersonation to obtain credit or secret information
 - Posing as the plaintiff's wife, or providing a father for a child on a birth certificate.
 - Etc.
- Must be use that shows that the name is in fact the plaintiff.
- The interest protected is a "proprietary" one.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

43

Prosser – Privacy

- The right to privacy is personal, not assignable, and generally does not survive death.
- Showing of special damages not required, but can increase damages if shown, or if punitive damages can be established.
- Public persons (defined page 119). Need "some logical connection between the plaintiff and the matter of public interest." p. 120.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

44



Student Presentation

Gaurav Narwani: The Future of Privacy in the Digital Age with the Rise of AI and IoT

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

45



Bloustein – Privacy as an Aspect of Human Dignity

A Response to Prosser:
The Human Dignity Thesis

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

46



Bloustein – Privacy as an Aspect of Human Dignity

- Feels that the varying cases on privacy have confused the underlying understanding which can cause issues for future cases.
- Takes issue with Prosser. In essence, Bloustein feels that we need to look at more than the remedy or particular interest affected.
- Feels that this moves us back to a tie to previously existing causes of action – like Thomson (cluster of rights).

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

47



Bloustein – Privacy as an Aspect of Human Dignity

- Says that Prosser steps away from Warren/Brandeis, who saw privacy as something larger, for which there is sometimes a cause of action.
- He says, however, that Warren/Brandeis never really defined it. pp. 161-162.
- Bloustein says “inviolate personality” encompasses the individual’s independence, dignity, and integrity.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

48

Bloustein – Privacy as an Aspect of Human Dignity



- Intrusion – he says Prosser “neglects the real nature of the complaint; namely that the intrusion is demeaning to individuality, is an affront to personal dignity.
- Says intrusion is “wrongful because [it is] demeaning of individuality, and [is] such whether or not [it] causes emotional trauma.” (which differs from Prosser). p. 165.
- For example, the 4th Amendment requires no such trauma.
- “Liberty of the person” underlies all intrusions.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

49

Bloustein – Privacy as an Aspect of Human Dignity



- Public Disclosure:

- Prosser improperly focuses on the particular harm, when the real issue is “that some aspect of their life has been held up to public scrutiny at all,” thus making it similar to the intrusion cases, since the publicity is a form of intrusion. Example p. 169.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

50

Bloustein – Privacy as an Aspect of Human Dignity



- Appropriation (page 173)
 - Again, no different than intrusion or public disclosure: not proprietary as suggested by Prosser, but a protection of individual dignity.
 - Same risk of harm from using a name for advertising and disclosing salacious details.
 - Only difference is the manner in which the dignity is harmed.
 - What about where the publication is a boon? Is it still a violation at first, and then consented in the future?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

51

Bloustein – Privacy as an Aspect of Human Dignity



- False Light:

- Addresses the “embrace” cases (“wrong kind of love” vs “right kind of love” articles). No indignity from mere republication without comment, because they consented by embracing in public.
- BUT, there was no consent to any further use in connection with a damaging statement – this turns it into a violation of dignity.
- Thinks Prosser missed it because he focused on the couple’s loss of commercial rights, not the harm to their individuality.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

52

Bloustein – Privacy as an Aspect of Human Dignity

- Bloustein says he's right because his theory holds when you get outside of torts, and Prosser's does not.
- 4th Amendment: is actually a protection of human dignity, and not concerned with prevention of emotional distress.
- *DeMay* (unauthorized witness to childbirth) and *Silverman* (wiretap) are premised on "an affront to the individual's independence and freedom."
- Same value in peeping tom statutes.



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

53

Bloustein – Privacy as an Aspect of Human Dignity

- Why does this matter?
 - Prosser's approach will have the tendency to deny relief where there has not previously been damage found. Same problem as *Roberson*.
 - Bloustein also changes the way you look at remedies, because it becomes a remedy to individuality, not reputation or some other already-recognized harm.



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

54

Palmer – The Three Milestones in the History of Privacy in the United States



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

55

Palmer – Three Milestones in Privacy in the US

- The US differs from Europe in its views of privacy rights.
 - In Europe, privacy is an inherent right related to an individual's social personality rights.
 - In the US, the law has developed over time to sweep together various liberties that are not traditionally "privacy" rights.
- "[P]rivacy in the United States is now an umbrella concept under which diffuse personality interests are brought together."
- Palmer does not dwell on defining "privacy" but believes that "privacy cannot be defined coherently to mean so many things."



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

56

Palmer – Three Milestones in Privacy in the US

- Palmer posits that we got where we are now based on three milestones in the past 120 years of privacy law creation:
 1. The Warren/Brandeis Article, "The Right to Privacy," in 1890.
 2. The Prosser Article, "Privacy," in 1960.
 3. US Supreme Court interpretation of liberty rights from 1960-present.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



57

Palmer – Three Milestones in Privacy in the US

1. Warren/Brandeis - "The Right to Privacy"

- Palmer takes a different view of the article and finds three "phases of the personality" that the article sought to protect (not just the "right to be let alone"):
 - Control over the use of one's name, likeness, or photograph.
 - A reserved sphere of personal and family life.
 - Control over one's creations, writings, and thoughts.
- They also "offered no doctrinal steps, constructed no new [laws] ... [f]uture steps are not even discussed. The solutions were simply entrusted to the judges."

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

58

Palmer – Three Milestones in Privacy in the US

2. Prosser - "Privacy"

- To Palmer, Prosser "lifted the confusion" about privacy that previously existed and persuaded the reader that "each tort had distinguishable characteristics, offered different protections, and did not duplicate or conflict with the other three."
- But Prosser also took "liberties" with the cases he read and "retrofit[ed] them to his purposes" to make the four categories.
- Also, while Prosser sought to find order in the chaos of privacy, his four torts have "nothing in common with each other".

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



59

Palmer – Three Milestones in Privacy in the US

3. Transformation of Liberty into Privacy

- Supreme Court started characterizing an "interest in independence in making certain kinds of important decisions" as a privacy right.
 - Included marriage, procreation, raising children, travel, etc.
- Not just the freedom to be private, but to make personal choices in public.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

60

Palmer – Three Milestones in Privacy in the US

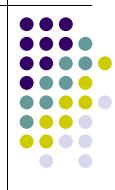


3. Transformation of Liberty into Privacy

- *Griswold v. Connecticut* – “zones of privacy” not explicitly defined in the US Constitution protect the marital relationship.
- *Roe v. Wade* – found a right to choose to terminate her pregnancy was part of her right to privacy.
- *Lawrence v. Texas* – found a freedom to choose a sexual lifestyle.
- As a result, “[m]any personality rights are recognized in the United States as if they were aspects of privacy.”

Moral and Legal Foundations of Privacy

February 14, 2023



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

1

III. Privacy and the Government

1. The Fourth Amendment



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

2

What Is the U.S. Constitution?



- A founding document of the United States that sets out the national framework of the U.S. government
 - Executive Branch
 - Legislative Branch
 - Judicial Branch
- Created in 1787; became effective 1789
- Has been amended 27 times since then, including the Bill of Rights in 1791 (Amendments 1-10)
 - These first ten amendments were largely prohibitions against government action in certain areas of life:
 - Freedom of speech, religion, and press, etc.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

3

The 4th Amendment to the U.S. Constitution



- **The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated,** and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
- Questions to ask:
 - Was the government involved?
 - Was there a search or seizure?
 - Was the search or seizure reasonable?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

4



Olmstead v. U.S.

Privacy over Physical Property Alone?

Presentation by: Aditya Gaur

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

5



Olmstead v. U.S. (1928)

- Defendant was engaged in bootlegging, the government tapped his telephone.
- The Court looks to the 4th Amendment and finds no violation:
 - “The [Fourth] Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the house or offices of the defendants. . . .”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

6



Olmstead v. U.S. (1928)

- The Court's analysis continues:
 - “The language of the [Fourth] Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

7



Olmstead v. U.S. (1928)

- “The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the 4th Amendment.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

8

Olmstead v. U.S. (1928)

- Brandeis dissents from the majority opinion:
 - Thinks the protection of the 4th Amendment is much broader than physical property, and includes “the right to be let alone.”
 - (This is the same Brandeis as the author of “The Right to Privacy” from last week)
 - To Brandeis, it is immaterial where the physical connection with the telephone wires leading into the defendants’ premises was made. And it is also immaterial that the intrusion was in aid of law enforcement.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

9

Katz v. United States

The Expectation of Privacy

Presentation by: Vinayak Khandelwal

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

10

Katz v. U.S. (1967)

- Government tapped a public telephone booth, and was allowed to introduce the recordings at trial.
- The Supreme Court reversed, finding that the 4th Amendment “protects people, not places.”
- Thus, it is immaterial that a phone booth is “public” if the person reasonably expects privacy in the content of the call – even if the booth is made of glass.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

11

Katz v. U.S. (1967)

- “One who occupies [the phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.”
- “To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

12

Katz v. U.S. (1967)

- The government argued that there was no physical intrusion into the phone booth.
- The Court disagreed: “the underpinnings of . . . [Olmstead] . . . have been so eroded by our subsequent decisions that the ‘trespass’ doctrine . . . can no longer be regarded as controlling.”
- “The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

13

Katz v. U.S. (1967)

- The Court finds the fact that the government was restrained in its action is of no matter, and its conduct cannot be “retroactively” validated.
- Justice Harlan’s concurrence:
 - Created what is now known as the “reasonable expectation of privacy” test.
 - “[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

14

Katz v. U.S. (1967)

- Justice Harlan’s concurrence:
 - “Thus a man’s home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the ‘plain view’ of outsiders are not ‘protected’ because no intention to keep them to himself has been exhibited.”
 - Here, in Katz’s case, the “critical fact” is that one who occupies a telephone booth, “shuts the door behind him, and pays the toll that permits him to place a call surely is entitled to assume that his conversation is not being intercepted. The point is not that the booth is ‘accessible to the public’ at other times, but that it is a temporary private place whose momentary occupants’ expectation of freedom from intrusion are recognized as reasonable.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

15

Katz v. U.S. (1967)

- Justice Black’s dissent:
 - He reads the 4th Amendment as written and says that it only protects tangible things from being searched and seized.
 - “A conversation overheard by eavesdropping, whether by plain snooping or wire-tapping, is not tangible” and thus “can neither be searched nor seized.”
 - If the Framers had wanted to prohibit eavesdropping, they would have used appropriate language in the 4th Amendment.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

16



Smith v. Maryland

The Third-Party Doctrine

Presentation by: Gaurav Narwani

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

17



Smith v. Maryland (1979)

- Local case from Baltimore in 1976.
- Patricia McDonough was robbed then later received threatening phone calls from someone who claimed to be the robber.
- The police found the man (Michael Smith) and had the telephone company install a pen register to record the numbers he dialed from his home phone.
- The register revealed that Michael Smith was calling Patricia McDonough.
- Smith was later arrested and at trial claimed the pen register was a violation of his 4th Amendment rights.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

18



Smith v. Maryland (1979)

- The Supreme Court starts by reviewing the *Katz* decision and its two conclusions:
 - The Fourth Amendment “protects people, not places.”
 - What matters is whether the person has a “reasonable expectation of privacy.”
- The Court then distinguishes over *Katz*.
 - “[A] pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications. ... Given a pen register’s limited capabilities, therefore, [Smith’s] argument that its installation and use constituted a ‘search’ necessarily rests upon a claim that he had a ‘legitimate expectation of privacy’ regarding the numbers he dialed on his phone.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

19



Smith v. Maryland (1979)

- The Court thus rejects Smith’s claim because it “doubt[s] that people in general entertain any actual expectation of privacy in the numbers they dial.”
- People have to realize that they “convey” phone numbers to the telephone company, since the telephone company has to set up the call.
- The telephone company also lists all of the numbers you call on your monthly bills.
- “Although most people may be oblivious to a pen register’s esoteric functions, they presumably have some awareness of one common use: to aid in the identification of persons making annoying or obscene calls.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

20

Smith v. Maryland (1979)

- The Court also finds that “the site of the call is immaterial.” While Smith made the call at home may have kept the “contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.”
- Thus the Court defines what is now known as the “third-party doctrine”:
 - A person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.
- The basis of the third-party doctrine is that the person disclosing the information “assumes the risk” that the third-party can disclose it to anyone.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

21

Smith v. Maryland (1979)

- If Smith had placed the call through an operator, he could claim no legitimate expectation of privacy.
- The Court sees this as no different than that situation. When Smith dialed the numbers he “assumed the risk that the [telephone] company would reveal to police the numbers he dialed.”
- Justice Stewart’s dissent:
 - Dialing numbers is inherently necessary for making phone calls, just as is talking into the phone.
 - Following the Court’s opinion, the conversation would no longer be private because it too “must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

22

Smith v. Maryland (1979)

- Justice Marshall’s dissent:
 - Even if the public knows of pen registers (and Justice Marshall doubts they do), “it does not follow that they expect this information to be made available to the public in general or the government in particular.”
 - “Privacy is not a discrete commodity, possessed absolutely or not at all.”
 - Justice Marshall rejects the “assumption of risk” argument.
 - If you disclose certain records to a bank or telephone company for a limited purpose, you need not assume the information could be used for other purposes.
 - If so, a person “cannot help but accept the risk of surveillance” unless one chooses to forego “personal or professional necessity,” like using the telephone.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

23

Hardee – Kyllo v. U.S.

Emerging Technologies

Presentation by: FNU Shruthi Duraisamy

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

24

Kyllo v. US (2001)

- Police used a thermal camera on Danny Kyllo's house in Oregon from an officer's car across the street.
- The camera showed that an unusual amount of heat was radiating from the roof over the garage and the side of his home.
- The officers concluded that this heat was from lamps used to grow marijuana in his house.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

25

Kyllo v. US (2001)

- The officers used the imaging information (and other things) to get a search warrant.
- The search led to officers finding more than 100 marijuana plants.
- Kyllo moved the court to suppress the seized evidence because it was obtained in violation of his Fourth Amendment rights.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

26

Kyllo v. US (2001)

- The trial court denied his motion.
 - Found no rays or beams enter house, "cannot penetrate walls or windows to reveal conversations or human activities."
- Kyllo appealed to the 9th Circuit (the intermediate appellate court).

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

27

Kyllo v. US (2001)

- 9th Circuit found that Kyllo had shown no subjective expectation of privacy because he made no attempt to conceal the heat escaping from the home
- Even if he had, he had "no objectively reasonable expectation of privacy" in the heat radiating from his house. The camera provided no private details, only amorphous hot spots.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

28

Kyllo v. US (2001)

- The Supreme Court found that there was a "search"
 - The camera obtained information that would otherwise not be obtained.
 - That the heat left the house was no different than the wiretap of a phone booth in Katz.
- The government argued that the search was proper because it did not detect private activities in private areas.
 - But support was from *Dow Chemical* case.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

29

Kyllo v. US (2001)

- Supreme Court (Scalia) held that:
 - (1) Use of sense-enhancing technology to gather any information regarding interior of home that could not otherwise have been obtained without physical intrusion into constitutionally protected area constitutes a "search," and
 - (2) Use of thermal imaging to measure heat emanating from home was search.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

30

Kyllo v. US (2001)

- "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant."

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

31

Thompson - U.S. v. Jones

GPS Tracking of a Vehicle

Presentation by: Xianglong Wang

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

32

US v Jones (2012)

- Police had a warrant to install a GPS device on Jones's vehicle within 10 days in DC.
- Police did not install until the 11th day and in Maryland.
- They tracked Jones's car for 28 days.
- Trial court granted motion to suppress evidence regarding position when vehicle was parked. Jones had no expectation of privacy while moving.

Privacy - Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

33

US v Jones (2012)

- Supreme Court:
 - 4th Amendment applies to vehicles, and using GPS to monitor movements is a search.
 - Attachment of the GPS device, coupled with its use to monitor Jones's movements, was a search.
 - Focuses on "in their persons, houses, papers and effects" from the 4th Amendment.
 - Jones's car is an "effect".
 - Government failed to argue that the search was reasonable, so that issue was not considered.

Privacy - Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

34

US v Jones (2012)

- Justice Sotomayor concurred, and discussed whether there is a reasonable expectation of privacy, even though that issue was not before the Court.
 - Also said we may need to reconsider privacy in information given to third parties in the digital age.
- Justice Alito and others said wrong to use physical attachment; *Katz* should be the rule.
 - Trespass neither "necessary nor sufficient" in *Katz*.

Privacy - Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

35

McCubbin - Carpenter v. U.S.

Cell Phone Location and Movement of Users

Presentation by: Zeyin Zhang

Privacy - Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

36

Carpenter v. US (2018)

- Background facts:

- Cellular service providers track and log the location and movement of modern cell phones constantly.
- This is called Cell Site Location Information ("CSLI").
- When a cell phone connects to cell towers, the towers record CSLI.
- The more towers in the area, the more precise the CSLI information is (precise to 0.5 to 2 miles).

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

37

Carpenter v. US (2018)

- In 2011, Detroit police arrested four people (including Carpenter) they thought had robbed several Radio Shack and T-Mobile stores in the area.
- The government requested cell phone location records from the cellular providers of Carpenter and the others (MetroPCS and Sprint).
- Did not seek the information under a warrant.
- The government received almost 13,000 CSLI for Carpenter (an average of 101 points per day).
- CSLI showed that Carpenter had been near the robbery locations.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

38

Carpenter v. US (2018)

- Chief Justice Roberts starts with the evolution of Fourth Amendment analysis through some of the cases we've analyzed in class.
- This case, and CSLI, however, do not "fit neatly under existing precedents" and is at the "intersection of two lines of cases": those related to geolocation and those related to the third-party doctrine.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

39

Carpenter v. US (2018)

- "Much like GPS tracking of a vehicle" (the *Jones* case), "cell phone location information is detailed, encyclopedic, and effortlessly compiled."
- It is "tireless and absolute surveillance", "near perfect surveillance, as if it had attached an ankle monitor to the phone's user."
- It "provides an all-encompassing record of the holder's whereabouts."

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

40

Carpenter v. US (2018)

- The Court finds a reasonable expectation of privacy in CSLI because “the time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’”
- CSLI presents an even greater privacy concern than GPS monitoring because a cell phone is almost “a feature of human anatomy”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

41

Carpenter v. US (2018)

- There has been a “seismic shift” in digital technology since the early Fourth Amendment cases that force the Court to reanalyze its previous analyses:
 - “There is a world of difference between the limited types of personal information addressed in” the early cases and that “casually collected by wireless carriers today.”
- Finds that the third-party doctrine (*Smith*) does not apply because of the amount of information collected and the “unique nature of cell phone records.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

42

Carpenter v. US (2018)

- Four dissenting opinions (which is a lot):
 - Justice Kennedy dissents primarily on the third-party doctrine, finding that cell-site records are no different from other records, like credit card records.
 - Finds that CSLI is not as accurate as Roberts believes.
 - Justice Thomas does not think any “property” of Carpenter has been searched. He believes CSLI is property of the wireless carriers.
 - Justice Alito’s dissent is along similar lines as Justice Thomas, but goes into details on warrants (which is outside the scope of this class).

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

43

Carpenter v. US (2018)

- Justice Gorsuch believes the Court overstepped its precedent in basically ignoring the third-party doctrine and *Smith* because the Roberts did not like the result.
- Justice Gorsuch says so what? “Live with the consequences” of having judicial precedent and following it, rather than creating new law.
- Instead, Justice Gorsuch believes that *Smith* and the third-party doctrine are “on life support.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

44

Moral and Legal Foundations of Privacy

February 22, 2023



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

1

Recap of Last Week



- What Are the Boundaries of the Fourth Amendment?
 1. Olmstead v. US – Early view that 4th Amendment only covers physical property
 2. Katz v. US – Rejection of Olmstead; “reasonable expectation of privacy” test
 3. Smith v. Maryland – Pen register case; third-party doctrine
 4. Hardee/Kyllo case – “Search” can be done without physical intrusion
 5. Thompson/Jones case – GPS tracking and “mosaic” theory
 6. McCubbin/Carpenter case – digital technology issues

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

2



III. Privacy and the Government

2. Digital Searches and Seizures

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

3



Moore - Riley v. California

Search of Cell Phones

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

4

Riley v. California (2013)

- Combination of two different cases with two different fact patterns.
- One case involved David Riley; the other involved Brima Wurie.
- Court combined them because they deal with the same legal issue: whether a search of cell phones is a violation of the 4th Amendment.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

5

Riley v. California (2013)

Riley:

- Riley stopped for traffic violation that led to arrest for weapons.
- As part of the arrest, an officer took Riley's cell phone from his pants and accessed information in the phone.
- The officer saw references to a street gang, which led to further examination of the phone by police later.
- Found images/videos that led to charges in a shooting and enhanced charges for gang affiliation.
- Riley moved to suppress phone evidence, but was denied.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

6

Riley v. California (2013)

Wurie:

- Wurie arrested after being observed in a drug sale.
- Officers took Wurie's phone and noticed it was receiving multiple calls from "my house" on the external screen.
- Officers opened phone, searched call log and traced the "my house" number to Wurie's apartment.
- Obtained a search warrant and found drugs, guns, and money. Charged him with drug and firearm offenses as related to home search.
- Wurie moved to suppress. Appellate court vacated relevant convictions.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

7

Riley v. California (2013)

- General rule: no warrantless search of digital information on cell phone seized from person arrested absent a specific exception to the warrant requirement.
- What exceptions are in play?
- The Court analyzes them...

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

8

Riley v. California (2013)

- Three applicable precedents:

1. A search incident to an arrest must be limited to the area within the arrestee's immediate control, where it is justified by the interests in officer safety and in preventing evidence destruction.
2. These risks of officer safety and evidence destruction are present in all custodial arrests.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

9

Riley v. California (2013)

3. Searches of a car are OK where the arrestee is unsecured and within reaching distance of the passenger compartment, or where it is reasonable to believe that evidence of the crime of arrest might be found in the vehicle.
 - Note – The Court explains that the second point, “reasonable to believe evidence of the crime or arrest might be found in the vehicle”, is based on “circumstances unique to the vehicle context,” presumably the lower expectation of privacy in a vehicle than of your person.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

10

Riley v. California (2013)

- Question: How does the “search incident to an arrest” doctrine apply to modern cell phones, which are so common that “the proverbial visitor from Mars might conclude they were an important feature of human anatomy”?
 - Technology didn’t exist when earlier cases were decided.
 - Digital content on cell phones doesn’t really fit with the rationales of the earlier cases where *physical* items were searched for their *physical contents*.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

11

Riley v. California (2013)

- The Court assessed “on the one hand, the degree to which [the search of the cell phone] intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.”
- The Court found that a search of *digital information* on a cell phone does not further the government interests of protecting officer safety and avoiding destruction of evidence, and implicates substantially greater individual privacy interests than a brief physical search.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

12

Riley v. California (2013)

Reasons for an insufficient legitimate government interest:

1. Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape.
2. A general concern regarding remote wiping/encryption isn't enough. There is less concern that the arrested person will be able to conceal or destroy evidence within his reach than for *physical evidence*.
 - In addition, no indication this is a common issue, or that search incident to arrest would solve the problem.
 - Technologies exist to respond to remote wiping.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

13

Riley v. California (2013)

- Intrusion is an issue because cellphones differ from other objects a person may carry.
 1. Capacity: Immense storage that "collects in one place many distinct types of information that reveal much more in combination than any isolated record."
 2. "...Even just one type of information to convey far more than previously possible."
 3. Longevity: Data can date back years.
 4. Pervasiveness: Many of the 90% of Americans with cell phones keep on their person a digital record of everything

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

14

Riley v. California (2013)

- The Court realizes this "will have some impact on the ability of law enforcement to combat crime," but does not mean police can never get the information:
 - They can get a warrant, which is becoming easier.
 - While this decision finds the "search incident to arrest" exception does not apply, others may allow for a warrantless search in particular cases, such as "exigent circumstances."

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

15

Andersen - U.S. v. Stanley

Privacy over Electronic Communications

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

16

U.S. v. Stanley (2014)

- Erdely (investigator) suspected that a number of files on a file-sharing network were child pornography based on the file titles (and confirmed that several were).
- Erdely obtained the network's globally unique identification (GUID) and the IP address for the computer sharing the information.
- Determined ISP was from Comcast, and obtained an order for Comcast to disclose.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

17

U.S. v. Stanley (2014)

- Conducted a search of the computers associated with the IP address, but those were not the computers.
- However, the resident used a wireless router and had an unsecured network, but had not given anyone permission to use the network.
- Resident allowed Erdely to access network and obtain private IP addresses/etc.
- Eventually obtained IP addresses.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

18

U.S. v. Stanley (2014)

- Erdely used a free version of Moocherhunter available online.
- MH enables use of a directional antenna to find out who is improperly accessing network.
- Used “passive mode” which requires entry of a MAC address for router, as opposed to searching.
- Can then trace signal to source.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

19

U.S. v. Stanley (2014)

- Erdely used Moocherhunter on resident's wireless router, and was able to trace the computer to its origin: Stanley's computer.
- Signal led across street to apartment complex; signal strongest at Stanley's apt.
- Erdely put all of this in a search warrant, which was granted for Stanley's residence.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

20

U.S. v. Stanley (2014)

- A federal grand jury returned a one-count indictment charging Stanley with possession of child pornography.
- Stanley moved to suppress for improper search/seizure.
- Stanley says information obtained in violation of 4th Amendment.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

21

U.S. v. Stanley (2014)

- Trial Court:
 - Stanley had a subjective and reasonable expectation of privacy in home under *Katz*.
 - BUT he did not for the files on his computer, especially given that he put them on a file-sharing network.
 - So, was use of Moocherhunter a search?
 - In other words, did Stanley have a legitimate expectation of privacy in his wireless signal?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

22

U.S. v. Stanley (2014)

- No reasonable expectation of privacy in information voluntarily conveyed to third parties per *Smith* case:
 - *Smith* was use of pen registers, which include the numbers dialed.
 - Different than *Katz* where the actual content of the conversation was monitored.
 - No expectation of privacy in the numbers dialed because they are “conveyed” to a third party – the phone company.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

23

U.S. v. Stanley (2014)

- Trial court says Stanley’s wireless signal is like a pen register in *Smith*.
 - Thus, no legitimate expectation of privacy, and use of MH to track that signal was not a search.
 - *Smith* tracked phone numbers conveyed to third parties, MH tracked signal strength sent to third parties.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

24

U.S. v. Stanley (2014)

- Stanley argued that this was a different situation than *Smith* because Moocherhunter is a tracking device.
- Court rules require a warrant for the use of a tracking device if it implicates a Fourth Amendment right.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

25



U.S. v. Stanley (2014)

- Trial Court disagrees;
 - Even if it was a tracking device, under *Kyllo*, it was generally available.
 - Different than the heat in *Kyllo* which was not directed outside – Stanley's signal was.
 - Stanley may have wanted to remain private, but that expectation was not reasonable given that he directed his information outside the home.
 - Had he not made unauthorized access to a wireless router, he would have been known.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

26



U.S. v. Stanley (2014)

- On appeal, the Third Circuit disagreed with the Trial Court's application of the "third-party doctrine."
 - Thought this application of the "third-party doctrine" too broad, because it would cover all Internet traffic, since all Internet traffic is shared with a third party (like a server).
 - Appeal Court was concerned that law enforcement would have "unfettered access" to Internet data without Fourth Amendment protection.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

27



U.S. v. Stanley (2014)

- The Third Circuit still upheld the conviction, though.
- Stanley did not have a reasonable expectation of privacy because of the "dubious legality" of using his neighbor's wireless signal.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

28





Solove and Schwartz – Digital Searches and Seizures

Searches and Seizures in a Digital World

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

29



Digital Searches & Seizures

- A collection of various topics and cases that relate to those topics, along with questions to stretch your thinking on each topic.

1. Searching Computer Contents
2. Encryption
3. E-mail
4. ISP Records
5. IP Addresses and URLs
6. Key Logging Devices

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

30



Digital Searches & Seizures

- 1. Searching Computer Contents:

- Generally, a generic search warrant for an entire computer system is enough for the government to find the “needle in a haystack.”
- It is no different than a search of an entire house for drugs.
- *US v. Campos* (2000): a warrant to look for one set of images found others. Court allowed the search because of the nature of searching computers.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

31



Digital Searches & Seizures

- There are limits to search warrants

- In *US v. Carey* (1999), a warrant to search a computer for drug information was not enough to search for pornography.
- Is copying a search and seizure under the 4th Amendment?
 - *US v. Gorshkov* (2001) did not think so.
 - Some commentators do.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

32

Digital Searches & Seizures

- What about password protection?
 - *Trulock v. Freeh* (2001) only allowed the search of the password-protected part of the computer consented for search
 - *US v. Andrus* (2007) allowed the search of an entire password-protected computer without consent
 - Compare *Trulock* and *Andrus*.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

33

Digital Searches & Seizures

- 2. Encryption:
 - *Junger v. Daly* (2000): encryption is protected free speech, at least in source code form.
 - *But see Karn v. US* (1996): regulation of encryption source code through export controls is a valid government purpose.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

34

Digital Searches & Seizures

- 3. E-mail:
 - *Steve Jackson Games v. US Secret Service* (1994): electronic BBS (a store and forward e-mail system). Warrant to search SJG and Blankenship residence; SJG warrant for computer data.
 - Was the unread e-mail obtained from the BBS an intercept without a court order?
 - No, because the e-mails were in storage, not in transmission, when obtained.
 - It was a violation of 18 USC 2701, though.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

35

Digital Searches & Seizures

- Carnivore:
 - FBI mechanism to intercept e-mail and IMs from ISP and capable of analyzing the entire e-mail traffic at an ISP.
 - Programmed only to search to/from (like pen register), but could do more if instructed.
 - Government said it was only searching pursuant to warrants, but who knows?
 - 2001 Patriot Act authorized Carnivore subject to some limitations.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

36

Digital Searches & Seizures

- 4. ISP Records:

- *US v. Hambrick* (1999)
 - An adult sought to entice minor online (the “minor” was a police officer).
 - Officers served subpoena on the adult’s ISP (Mindspring) to get his name. Mindspring complied.
 - Warrant was invalid because of interested judge.
 - Should the information be suppressed for violation of the Fourth Amendment?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

37

Digital Searches & Seizures

- Court looks to see if defendant had a “reasonable expectation of privacy”:
 - 1. Subjective expectation of privacy
 - 2. Objectively reasonable expectation of privacy
- Key in this case is whether there was “objectively reasonable” expectation.
- Court says no. Hambrick was not completely anonymous because the ISP knew who he was. Nothing in their agreement to the contrary.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

38

Digital Searches & Seizures

- “Where such dissemination of information to nongovernment entities is not prohibited, there can be no reasonable expectation of privacy in that information.”
- The Court relies on *Smith v. Maryland* and the third party doctrine to come to this conclusion.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

39

Digital Searches & Seizures

- 5. IP Addresses/URLs:

- *US v. Forrester* (2008): Defendants convicted of running ecstasy lab appeal because use of a “mirror port” to monitor e-mail and tracking Internet activity violated the 4th Amendment.
- The Court relies on *Smith v. Maryland*, finding use of pen registers for phone numbers is not a search, because no reasonable expectation of privacy in that kind of information.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

40

Digital Searches & Seizures

- Court says that “mirror ports” and pen registers are constitutionally the same, and thus no expectation of privacy –
 - (1) users know the to/from information in an e-mail will be given to third parties to convey the information; and
 - (2) it provides no information about the substance of the transmission.
- After this case, the 2001 Patriot Act confirmed that the Pen Register Act applied to e-mails.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



41

Digital Searches & Seizures

- 6. Key Logging Devices
 - US v. Scarfo (2001): during a search, government found computer with encrypted “Factors” file, and installed a “Key Logger System” to gain access information.
 - Court was concerned that government intercepted information over telephone wires without applying for a wiretap.
 - Scarfo said it was a violation because it collected data on all keystrokes, not just the passphrase to the “Factors” file.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

42

Digital Searches & Seizures

- Court looks at the search warrant and said it was very specific.
 - Moreover, that KLS recorded other kinds of keystrokes doesn't turn the limited search into a general exploratory search.
 - Compares to searching in a closet or filing cabinet.
- Court said no wiretap issue because the software was designed not to record keystrokes when the modem was operating, so the KLS could not “intercept” communications.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



43

III. Privacy and the Government

3. National Security

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

44

Solove – I've Got Nothing to Hide

The “I've Got Nothing to Hide” Argument Against Privacy

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



45

Solove – Nothing to Hide

- The government's surveillance over you continues to grow as part of the war on terror:
 - NSA warrantless wiretapping
 - Total Information Awareness (TIA)
 - NSA review of phone and bank records
- There has been some public outcry, but most just shrug and say “I've got nothing to hide”
- Is that a sufficient answer?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

46

Solove – Nothing to Hide

- This is not limited to the US; in the UK, CCTV is everywhere, and the government markets it using the “nothing to hide” argument:
 - “If you've got nothing to hide, you've got nothing to fear”
- To someone like Solzhenitsyn, though, “Everyone is guilty of something or has something to conceal. All one has to do is look hard enough to find what it is.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



47

Solove – Nothing to Hide

- But many people are willing to exchange “a small amount of privacy for a potential national security gain.”
- The “nothing to hide” argument is then just a balance of the relative values of privacy and security, and favors security over privacy.
- Does it make a difference in your mind if it is just a computer doing the collecting and analysis? It limits human eyes on information.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

48

Solove – Nothing to Hide

- Solove thinks the “nothing to hide” argument is flawed.
- This stems, in part, from his belief that the “third-party doctrine” in the Fourth Amendment cases is incorrect and should be changed.
 - “[T]he lack of Fourth Amendment protection of third party records results in the government’s ability to access an extensive amount of personal information with minimal limitation or oversight.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

49

Solove – Nothing to Hide

- “Surveillance can create chilling effects on free speech, free association, and other First Amendment rights essential for democracy. Even surveillance of legal activities can inhibit people from engaging in them.”
- “Chilling effects harm society because, among other things, they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

50

Solove – Nothing to Hide

- To Solove, aggregation surveillance (like what the NSA does) is a problem because it is “suffocating” and “aims to be predictive of behavior, striving to prognosticate about our future actions.”
- The other problem is “exclusion,” that this collection and these programs are kept secret from us.
- What else will the government do with the information in the future as yet unrevealed to us?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

51

Solove – Nothing to Hide

- Some critics believe that privacy problems are not very compelling because they do not have “enough dead bodies.”
 - But what about Rebecca Shaeffer and Amy Boyer? Both killed by stalkers who gained personal information about them from databases.
- Solove says this objection is similar to the “nothing to hide” argument. He believes there is still a harm worth addressing, even if it is not sensational.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

52

Solove – Nothing to Hide

- To Solove, a general security interest should not be weighed against a general privacy interest.
- Instead, we should limit the government collection by “judicial oversight” and “minimization procedures.”
- “Only in cases where such procedures will completely impair the government program should the security interest be weighed in total, rather than in the marginal difference between an unencumbered program versus a limited one.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

53



Global Relief Foundation v. O’Neill

FISA and the FISC

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

54



Global Relief v. O’Neill (2002)

- Background facts:
 - Global Relief is a non-profit and claims to support humanitarian relief programs throughout the world.
 - After the 9/11 attacks, the FBI looked to Global Relief and its potential connections to the terrorists who carried out the attacks.
 - The FBI searched Global Relief’s HQ pursuant to the Foreign Intelligence Surveillance Act (“FISA”).
 - Global Relief challenged the search as illegal and in violation of the Fourth Amendment.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

55



Global Relief v. O’Neill (2002)

- FISA:
 - Law passed by Congress in 1978 to create a framework in which the government can conduct “legitimate electronic surveillance for foreign intelligence purposes” while recognizing “privacy and individual rights.”
 - The FISA created an oversight special court called the Foreign Intelligence Surveillance Court (“FISC”), which reviews applications for authorization of electronic surveillance (similar to a search warrant).
 - The FISA requires the government to provide certain information in support of its application for surveillance.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

56



Global Relief v. O'Neill (2002)

- The government must provide:
 - Facts to justify belief that the target of the search is a foreign power or an agent of a foreign power.
 - Premises to be searched contains foreign intelligence information.
 - Information sought is foreign intelligence information that could not reasonably be obtained through normal investigative means.
- If the target of the search is a “United States person,” there must also be probable cause and procedures to minimize intrusion.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

57

Global Relief v. O'Neill (2002)

- FISA also allows for surveillance without a warrant in “emergency situations” as long as the government later applies for a warrant within 72 hours of the initial search.
- In this case, the Court found that the US Attorney General had declared such an “emergency situation” and had later applied for a warrant within the 72-hour window.
- Thus, the search of Global Relief’s HQ was authorized under FISA.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

58

Global Relief v. O'Neill (2002)

- The Court also found no Fourth Amendment concern.
- “FISA’s safeguards provide sufficient protection for the rights guaranteed by the Fourth Amendment in the context of foreign intelligence activities.”
- Because the government followed the FISA requirements, the Fourth Amendment was not violated.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

59

Klayman v. Obama

NSA Surveillance and Telephone Metadata

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

60

Klayman v. Obama (2013)

- Background facts:

- 2013 Snowden revelations that the NSA was conducting widespread wiretapping and data collection of the public. The government was:
 - (1) Targeting non-US persons outside the US by surveillance occurring in the US.
 - (2) Collecting telephone metadata.
 - (3) Spying on foreign countries and their leaders.
 - (4) Attempting to weaken encryption standards.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

61

Klayman v. Obama (2013)

- Under the Obama administration, “the communication records of millions of US citizens [were] being collected indiscriminately and in bulk—regardless of whether they are suspected in any wrongdoing.”
- The plaintiffs filed this case against the government for violating various constitutional rights, including the Fourth Amendment and for violating FISA.
- After reviewing the history of FISA and the FISC, the court reviews the facts of the case.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

62

Klayman v. Obama (2013)

- The government’s “Bulk Telephony Metadata Program” collected information about the phone numbers used to make and receive calls, when the calls took place, and how long the calls lasted.
- The government did not collect any information about the contents of the calls or the name, address, or other information about the parties to the calls (other than their phone numbers).
- The government used this information to attempt to identify connections between terrorists.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

63

Klayman v. Obama (2013)

- The government’s collection had been happening for more than 7 years (2006-2013) and had been collecting from many telecom companies.
- The NSA then aggregated all the information into a single database to create a “historical repository that permits retrospective analysis.”
- The FISC had authorized this program, but only for “counterterrorism purposes.”
- The NSA limited its searches to three “hops” from a seed.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

64

Klayman v. Obama (2013)

- Fourth Amendment Analysis

- Threshold issue is whether the plaintiffs had a “reasonable expectation of privacy.”
- The Court starts with *Smith v. Maryland* and the third-party doctrine.
- The *Smith* case is much different than these facts, though.
- “When present-day circumstances—the evolutions in the Government’s surveillance capabilities, citizens’ phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court 34 years ago,” does *Smith* still apply?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

65

Klayman v. Obama (2013)

- The Court believes the metadata collection “almost certainly does violate a reasonable expectation of privacy” for several reasons:

1. Pen register in *Smith* was only for a few days and no expectation the government would retain the records.
2. Relationship between the police and the telephone company in *Smith* is “*nothing* compared to the relationship that has apparently evolved over the last seven years between the Government and telecom companies.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

66

Klayman v. Obama (2013)

3. The technology enables the government to “store and analyze the phone metadata of every telephone user in the US” and that makes it “unlike anything that could have been conceived in 1979.”
4. “[N]ot only is the government’s ability to collect, store, and analyze phone data greater now than it was in 1979, but the nature and quantity of the information contained in people’s telephony metadata is much greater, as well.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

67

Klayman v. Obama (2013)

- “This rapid and monumental shift towards a cell phone-centric culture means that the metadata from each person’s phone ‘reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.’”
- “Whereas some may assume that these cultural changes will force people to ‘reconcile themselves’ to an ‘inevitable’ ‘diminution of privacy that new technology entails,’... I think it is more likely that these trends have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as reasonable.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

68

Klayman v. Obama (2013)



- Court also finds the metadata collection an “unreasonable” search because the government does not have an immediate concern and the collection has not met any such terrorism concern.
- The government could not cite a single instance where the metadata collection stopped an imminent attack or aided a time-sensitive government objective.



Moral and Legal Foundations of Privacy

February 28, 2023

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

1



IV. Privacy in the Digital Age

1. Practical Implications

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

2



EFF – Governments Haven't Shown Location Surveillance Would Help Contain COVID-19

COVID-19 and Privacy

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

3



EFF – COVID-19 and Privacy

- March 2020 article from EFF at the beginning of the pandemic in the U.S.
- Article touches on location surveillance and the Fourth Amendment issues discussed in class so far.
- Governments are interested in containing COVID-19, but EFF believes that one measure, location surveillance, violates individual privacy and other rights.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

4

EFF – COVID-19 and Privacy

- China:
 - Built new infrastructures to track movement of massive numbers of identifiable people.
- Israel:
 - Used cellphone location data to identify people who came in close contact with virus carriers.
 - Sent quarantine orders based on this surveillance.
 - Other countries are testing a similar spying tool.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



5

EFF – COVID-19 and Privacy

- United States:
 - Government is seeking de-identified mobile app location data to predict the next virus hotspot.
 - Facebook has made similar data available in the past to track population movement during natural disasters.
- EFF believes that the de-identified data can easily be re-identified.
 - “One of the things we have learned over time is that something that seems anonymous, more often than not, is not anonymous, even if it’s designed with the best intentions.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

6

EFF – COVID-19 and Privacy

- EFF is concerned that governments appear to be creating these programs in secret.
 - “[N]ew surveillance powers must always be necessary and proportionate” but “we can’t balance those interests” without knowing what the new surveillance powers are.
- EFF thus lays out four questions that it believes are important in considering any surveillance related to COVID-19.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



7

EFF – COVID-19 and Privacy

1. Are the location records sought sufficiently granular to show whether two people were within transmittal distance of each other?
 - CSLI is only accurate to **0.5 to 2 miles** in urban areas.
 - GPS is accurate to a **16-foot** radius.
 - But health professionals recommend a radius of **6 feet** for social distancing.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

8

EFF – COVID-19 and Privacy

2. Do the cellphone location records identify a sufficiently large and representative portion of the overall population?
- Not everybody has a cell phone.
 - Older people are at higher risk of COVID-19, but tend not to have cell phones.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



9

EFF – COVID-19 and Privacy

3. Has the virus already spread so broadly that contact tracing is no longer a significant way to reduce transmission?
- Should the government thus divert its resources away from location tracking and toward other containment methods, like widespread testing?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

10

EFF – COVID-19 and Privacy

4. Will health-based surveillance deter people from seeking health care?
- According to the EFF, there are already reports that people subject to COVID-based location tracking are altering their movements to avoid embarrassment.
 - If a positive COVID test leads to enhanced location surveillance, some people may avoid getting tested.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



11

Lever – Privacy Faces Risk in Tech-Infused Post-COVID Workplace

COVID-19 and Privacy

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

12

Lever – Post-COVID Workplace



- Recent (February 2021) article that explores the potential privacy implications when people return to work in a post-COVID world.
- New technologies when they return:
 - Temperature checks
 - Distance monitors
 - Digital “passports”
 - Wellness surveys and health metric apps
 - Robotic cleaning/disinfection systems

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

13

Lever – Post-COVID Workplace



- “Digital health passes”
 - Salesforce/IBM
 - Clear
- Fitbit – “Ready to Work” program
- Microsoft/United Healthcare – “ProtectWell” app
- Amazon – “Distance Assistant”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

14

Lever – Post-COVID Workplace



- These systems “blur the lines between people’s workplace and personal lives … It erodes longstanding medical privacy protections for many different workers”
- “The invasion of privacy that workers face is alarming, especially considering that the effectiveness of these technologies in mitigating the spread of COVID-19 has not yet been established.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

15

Lever – Post-COVID Workplace



- Many companies are using third-party vendors to host the data and keep it separate.
- But many of these vendors have a business model centered on monetizing personal data.
- It’s all about a balance, the article concludes:
 - Employers have a legitimate interest in safeguarding workplaces and keeping employees healthy, but technologies are unproven.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

16



Data captured in the COVID Health Check will be retained for 30 days and may be used to initiate a case investigation with the JHCCC. De-identified aggregation of data (number of users engaging with system, response rates, etc.) will be used for system monitoring and improvement. The Johns Hopkins Prodenity mobile app will also follow basic security guidelines such as:

- Storage of data resides within an IT@JH managed environment either on-site or within the Microsoft Azure platform. Johns Hopkins has previously negotiated data privacy terms to utilize Azure for hosting of sensitive data (including HIPAA and FERPA).
- All data are protected as other sensitive data are protected, which includes (but is not limited to): encryption of data in transmit and at rest, strong authentication to access data, regular network scans to identify potential vulnerabilities, and data backed up securely in the event of an outage or other interruption of service.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

17



Solove – The Rise of the Digital Dossier

Is Your Personal Information Really Yours?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

18



Solove – Digital Dossier

- Short history of public-sector databases:**
 - Growth of the census.
 - Use of punch-cards and then computers allowed for processing of much more, and therefore collection of much more.
 - Led to privacy issues coming up in the 60s.
 - The Internet led to exponential growth – there are now* about 2,000 federal databases, and many state databases, all with important and sensitive personal data.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

19



Solove – Digital Dossier

- Short history of Private-sector databases:**
 - Personal marketing gave way to mass marketing, but only a small percentage purchased.
 - Led to “targeted marketing”, i.e. finding out which people were most likely to consume a product and focus on them.
 - The GM example (targeted marketing to Ford owners).
 - Direct marketing, telemarketing.
 - The 2% rule (only 2% of those contacted by direct marketing actually respond)**

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

20

Solove – Digital Dossier

- The more and better your data, the more targeted you can be.
 - Matching of census cluster data to phone books, etc.
 - Analytics of the data to understand traits of people.
 - We now get 500 pieces of mailings per year.
 - BUT, \$10 in sales for every \$1 in cost – double the rate of television.
- Now there is the database industry, that seeks to collect, analyze and sell personal information.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

21

Solove – Digital Dossier

- Companies can do this because of the fact we must “plug in” to various companies, and they maintain records on use.
- Creating new and different kinds of databases for all sorts of purposes – see examples on pages 21-23.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

22

Solove – Digital Dossier

- Two kinds of collection: direct solicitation of information and secret tracking.
 - Cookies – Doubleclick targeted advertising.
 - Web bugs – code that collects data; some can look at files.
 - Spyware – usually deceptively and secretly installed.
 - DRM that tracks information about copyrighted materials.
 - Bots – computer programs that troll the Internet looking for information.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

23

Solove – Kafka and Orwell: Reconceptualizing Information Privacy

Does Dystopian Literature Hold Some Truth?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

24

Solove – “Kafka and Orwell”

- Two metaphors – 1984 and “The Trial”
- 1984 – Orwell’s telescreen is similar in many respects to the Internet – you don’t know if or when information is being collected.
- But the Orwell metaphor has limits – data collections is in many respects ad hoc, and often for benign purposes.
- Goal of data marketers is to observe and exploit, not necessarily control. (True?)

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



25

Solove – “Kafka and Orwell”

- Solove says the main difference from 1984 is that marketers are interested in aggregate data, “not snooping into particular people’s private lives.”
- Solove’s article is from 2004. Is that true now? What is ever true? Even if not “human” observation, does the immediacy of it matter?
- What about knowing that there could be hacking by third parties?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

26

Solove – “Kafka and Orwell”

- Kafka
 - Joseph K awakes to find he is “under arrest” though he knows not why or by whom. The police do not know, and after telling him, leave.
 - JK spends the rest of the story trying to figure out why he was arrested and what will happen.
 - Finds there is a large dossier that is kept, that is passed among various courts for many years.
 - He is interrogated, but only if convenient. The Court loses interest, but JK becomes obsessed with the issue.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



27

Solove – “Kafka and Orwell”

- JK never seems to get any closer to figuring it out.
- In the end, he is seized by two officials and executed.
- Solove thinks Kafka better captures the issues related to databases through its insights rather than accurate depiction of today.
 - “sense of helplessness, frustration, and vulnerability” regarding entities that have control over a vast dossier of your information.
 - At any time, something could happen. Decisions are made based on the data, and we don’t have a say, knowledge, or the ability to fight back.
- Thus, the primary Kafka metaphor points to problems in the way entities treat individuals and their information.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

28

Solove – “Kafka and Orwell”

- Bureaucracies subject personal information to a process with little or no control or limit, which can limit “goals, wants, and needs.” Kafka shows how an imbalance in power, separate from any attempt to control, creates problems. He posits the same is true for databases.
- He recognizes (a little) that there may be an Orwellian component, i.e. targeted observation.
- Also, what about the compilation and cross-referencing of seemingly innocuous data? – the “Secrecy Paradigm”
- “Aggregation Effect” – a comprehensive collection is more than the sum of its parts.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

29

Solove – “Kafka and Orwell”

- What about inaccuracies? Solove provides examples...and then there's this:
 - <http://www.cbsnews.com/news/social-security-identity-fraud-scott-pelley-60-minutes/>
- Solove then provides various other problems:
 - “Impoverished Judgments”
 - “Powerlessness and Lack of Participation”
 - “Problematic Information Gathering Techniques”
 - “Irresponsibility and Carelessness”
- In sum, per Solove, we're heading to Kafka world.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

30

Rosen – The End of Forgetting

Once it Goes on the Web, It's There Forever

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

31

Rosen – The End of Forgetting

- Stacy the “Drunken Pirate.”



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

32

Rosen – The End of Forgetting



- Stacy the “Drunken Pirate.”
 - Denied a teaching degree for photo on MySpace showing her at a party and drinking from a plastic cup under the caption “drunken pirate.”
 - She sued for violation of First Amendment, but court denied, finding she was a public employee and the photo did not relate to matters of public concern, and therefore not “free speech.”
 - (also not entirely true...)

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

33

Rosen – The End of Forgetting



- It matters: 75% of employers do on-line searches, and 70% have rejected candidates.
- America in particular was the place you could disappear and reinvent yourself; not anymore...
- Online information makes it harder to have the “different selves” we’ve discussed in prior classes, since they all get muddled together on the Internet.
- And the Internet never forgets...

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

34

Rosen – The End of Forgetting



- Options?
 - Technological
 - Legislative
 - Judicial
 - Ethical
- As with most things, the answer is likely “all of the above,” but consideration of each is important.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

35

Rosen – The End of Forgetting



- ReputationDefender
 - Can monitor, and even help to fix an issue, but would likely become cost and time prohibitive when faced with “aggregator” technologies
 - Includes facial recognition technology we’ll discuss later...
- “Reputation Bankruptcy?": like financial bankruptcy – every 10 years or so could wipe out certain information.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

36

Rosen – The End of Forgetting



- Make it illegal for employers to refuse to hire or fire based on legal off-duty conduct revealed in Facebook, et al.?
 - NY, CA, CO, and ND already broadly prohibit employers from discriminating for legal off-duty conduct like smoking.
- Good old Lawsuits?
 - Even if you win a libel suit, no requirement to take the information down.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

37

Rosen – The End of Forgetting



- Should we create a right to demand retraction of false or damaging statements?
- But that doesn't address true information that's just embarrassing.
 - Solove suggests a "breach of confidence" suit if someone shares embarrassing photos/posts in violation of your privacy settings.
 - Raises serious First Amendment concerns.
- So, how about technological approaches?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

38

Rosen – The End of Forgetting



- Built-in expiration dates for data
 - Apps that delete texts after a period of time.
 - Apps that embed encryption in the data so that the key "rusts" and eventually doesn't work.
- Facebook thinks the opposite, namely that it has an obligation to reflect "current societal norms" that favor exposure over privacy.
- So what about "societal norms"?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

39

Rosen – The End of Forgetting



- People currently support requiring deletion of data and letting people know what websites know about them.
- Is that why we never "forgive and forget" for online information?
 - Would privacy nudges work?
 - MailGoggles (solving simple math problems before you can send emails at "late" hours)?
- Do we need to reconsider the "reasonable expectation of privacy" for the web?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

40

Rosen – The End of Forgetting



- Or, over time, will society just simply not take the Drunken Pirate seriously?
- What are some of the more recent efforts to address privacy online?
 - Snapchat, others?

Moral and Legal Foundations of Privacy

March 7, 2023



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

1



IV. Privacy in the Digital Age

1. Practical Implications

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

2



Polonetsky – 10 Privacy Risks and 10 Privacy Enhancing Technologies

Privacy Issues on the Horizon

Presentation by: Avradipta Das

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

3



10 Privacy Risks & Techs

- Whitepaper put together by the Future of Privacy Forum for “Data Privacy Day 2020.”
- “Technological advances are creating data protection challenges. But ultimately, managing key issues will continue to require trained people at the center of organizations to bring the human dimension to review products and services, to assess bias, to demand fairness, and to manage the systems and tools that can handle data protection at scale.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

4

10 Privacy Risks & Techs

Privacy Risk #1: Biometric Scanning

- A shift away from keyboard-based GUIs to biometric-enabled UIs.
- These UIs require companies to apply traditional data protection and privacy principles, but will “further blur the divide between law enforcement and consumer privacy concerns.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



5

10 Privacy Risks & Techs

Privacy Risk #3: Social Credit & Reputation Scoring Systems

- Ranking of individuals based on information gathered from social media.
- Social credit scores and analyses “span services and platforms, sweeping in a much broader array of unexpected information about an individual.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

6

10 Privacy Risks & Techs

Privacy Risk #4: Internet of Bodies & Brain-Machine Interfaces

- Like the IoT, but for medical and biometric devices inside our bodies connected to the Internet.
- “These more intimate devices raise a number of legal, ethical, and security challenges, including who should have access to the data they generate, how to mitigate the risks of malicious hacking, how to apply existing legal frameworks, and who is liable for vulnerabilities, malfunctions, or breaches.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute



7

10 Privacy Risks & Techs

Privacy Risk #6: Location Services & Proximity Tracking

- 5G signals have shorter range, which requires more cellular towers, which in turn increases location accuracy of data like CSLI.
- This takes the *Carpenter* case from before spring break to a new level.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

8

10 Privacy Risks & Techs

- “Many of the opportunities offered by emerging technologies relate to increased speed, efficiency, productivity, commercial output, and connectivity. To the extent that these benefits rely upon more extensive collection and processing of personal data, they pose data protection and security challenges.”
- Lists 10 “technological innovations and techniques that may be useful tools to manage privacy risks.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

9

10 Privacy Risks & Techs

- Technological innovations include:
 - Advances in Cryptography;
 - Localization of Processing; and
 - Advances in artificial intelligence and machine learning.
- Short-term actions can be taken by browsers, operating systems, and platforms, too.
 - “[A]s of January 2020, every leading browser has strictly limited or committed to limit most third party cookie tracking, a staple of today’s data ecosystem.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

10

IV. Privacy in the Digital Age

2. Privacy of Personal Data

a. Privacy Policies

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

11

Do People Really Understand Privacy Issues?

Stanley – Three Common Privacy Misconceptions that Companies Love

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

12

3 Privacy Misconceptions

- ACLU opinion paper on three common privacy misconceptions “that privacy-invading companies love.”
 1. “We care about your privacy!”
 2. What is unfair is also illegal
 3. We’ve lost the privacy battle

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

13

3 Privacy Misconceptions

1. “We care about your privacy!”
 - Nearly 60% of Americans believe that a website that has a privacy policy means that it will not share your information without your permission.
 - This is not accurate. Most privacy policies detail exactly how your data can be used.
 - “How We Use Your Data” would be a better name for these documents.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

14

3 Privacy Misconceptions

2. What is unfair is also illegal
 - “People have fairly well-defined feelings about what kinds of behavior are fair and what are not—and they tend to think that things that are unfair are also illegal.”
 - Large percentages of people (detailed in the article) misunderstand what online advertisers can do with personal data.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

15

3 Privacy Misconceptions

2. What is unfair is also illegal
 - So why do people give up so much info?
 - “The bottom line for us is resignation. It’s not as if people want to give up their privacy, but in order to get through life they feel they have to, and they don’t feel like they have the ability to change things.”

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

16

3 Privacy Misconceptions

3. We've lost the privacy battle

- Basically, there's nothing we can do about it.
- But there have been laws enacted recently to help combat privacy violations:
 - Europe's General Data Protection Regulation (GDPR)
 - California Consumer Privacy Act (CCPA)

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

17

Do People Really Understand Privacy Policies?

Litman-Navarro – We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

18

We Read 150 Privacy Policies

- Analysis of privacy policies from 150 popular websites and apps.
- Analyzed the length and readability (complexity) of each, and plotted the results on several graphs.
- Privacy policies took between 2 minutes (Craigslist) and 35 minutes (Airbnb) to read.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

19

We Read 150 Privacy Policies

- Found that most privacy policies exceeded a high school reading level, and many even exceeded a college reading level.
- For example, Facebook's privacy policy was much more difficult to read than a number of classic texts, like "Great Expectations" and "Pride and Prejudice."

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

20

We Read 150 Privacy Policies



- This means “a significant chunk of the data collection economy is based on consenting to complicated documents that many Americans can’t understand.”
- Contrasts BBC’s “unusually readable privacy policy” with Airbnb’s “particularly inscrutable” one.
- Shows the evolution of Google’s privacy policy over two decades.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

21

We Read 150 Privacy Policies



- “You’re confused into thinking these are there to inform users, as opposed to protect companies. These documents are created by lawyers, for lawyers. They were never created as a consumer tool.”
- Two things that will continue to make privacy policies more complicated:
 - More sophisticated and invasive data collection practices; and
 - Additional data protection laws (like California’s) with jurisdiction-specific addendums.
- Provides tips to make privacy policies more useful.

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

22

Privacy Policy Group Discussion



Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

23

Privacy Policy Discussion



- Split into three groups:
 - Breakout Room 1 – AirBnB Privacy Policy
 - Breakout Room 2 – Facebook Privacy Policy
 - Breakout Room 3 – TikTok Privacy Policy
- Work together as a group to answer three questions:
 1. On a scale of 1 (very easy) to 5 (very difficult), how difficult is it to understand the privacy policy?
 2. What kinds of data are shared about you, and with whom does the company share that data?
 3. Do you have any ability to limit the amount or types of data collected about you? If so, what steps do you have to take to do that?

Privacy – Spring 2023
© Matthew B. Welling

Johns Hopkins University
Information Security Institute

24



Mid-Term Review

Privacy – Spring 2023
© Matthew B. Weiling

Johns Hopkins University
Information Security Institute

25



[Help Center](#) > [Terms and policies](#) > [Privacy Policy](#) > Privacy Policy

About Airbnb

Your account

Safety and accessibility

Terms and policies

Terms of Service

Payments Terms of Service

Privacy Policy

Privacy Policy Supplements

Member policies and standards

Stays terms and policies

Airbnb Experiences terms and policies

Other terms and policies

Legal resources

Money Transmission License Disclosures

Privacy Policy

Last Updated: October 30, 2020

Airbnb exists to help build connections between people and make the world more open and inclusive. In short—to build a world where anyone can belong anywhere. We are a community built on trust. A fundamental part of earning that trust means being clear about how we use your information and protect your human right to privacy.

This Privacy Policy describes how Airbnb, Inc. and its affiliates (“**we**,” “**us**,” or “**Airbnb**”), process personal information that we collect through the Airbnb Platform. Depending on where you live and what you are doing on the Airbnb Platform, the supplemental privacy pages listed below may apply to you. Please follow the links and review the supplemental information provided there with information about how we process personal information for those regions and services.

IMPORTANT SUPPLEMENTAL INFORMATION

 **IMPORTANT SUPPLEMENTAL INFORMATION**

Outside of the United States. If you reside outside of the United States, such as in the European Economic Area (“**EEA**”) visit our “[Outside of the United States](#)” page to learn about (i) the controller(s) of your personal information; (ii) legal bases, including legitimate interests, for collecting and processing your personal information, (iii) safeguards relied upon for transferring personal information outside the EEA; (iv) your rights, and (v) contact details of the controller(s) and Data Protection Officer.

California and Vermont. If you reside in California or Vermont, visit our “[California and Vermont](#)” page to learn about specific privacy information that applies to you.

China. If you reside in the People’s Republic of China, which for purposes of this Privacy Policy does not include Hong Kong, Macau and Taiwan (“**China**”), visit our “[China](#)” page to learn about your rights and other specific information that applies to you.

Enterprise Customers and Airbnb for Work. If you use our enterprise services or have linked your account with an Airbnb for Work customer, visit our “[Enterprise Customers and Airbnb for Work](#)” page to learn about specific privacy information that applies to you.

1. DEFINITIONS

Undefined terms in this Privacy Policy have the same definition as in our [Terms of Service](#) (“**Terms**”).

2. PERSONAL INFORMATION WE COLLECT

2.1 Information needed to use the Airbnb Platform.

We collect personal information about you when you use the Airbnb Platform. Without it, we may not be able to provide you with all services requested. This information includes:

- **Contact Information, Account, Profile Information.** Such as your first name, last name, phone number, postal address, email address, date of birth, and profile photo, some of which will depend on the features you use.
- **Identity Verification and Payment Information.** Such as images of your government issued ID (as permitted by applicable laws), your ID number or other [verification](#) information, bank account or payment account information.

2.2 Information you choose to give us.

You can choose to provide us with additional personal information. This information may include:

- **Additional Profile Information.** Such as gender, preferred language(s), city, and personal description. Some of this information as indicated in your account settings is part of your public profile page and will be publicly visible.

- **Address Book Contact Information.** Address book contacts you import or enter manually.
- **Other Information.** Such as when you fill in a form, add information to your account, respond to surveys, post to community forums, participate in promotions, communicate with our customer care team and other Members, or share your experience with us. This may include health information if you choose to share it with us.

2.3 Information Automatically Collected by Using the Airbnb Platform and our Payment Services.

When you use the Airbnb Platform and Payment Services, we automatically collect personal information. This information may include:

- **Geo-location Information.** Such as precise or approximate location determined from your IP address or mobile device's GPS depending on your device settings. We may also collect this information when you're not using the app if you enable this through your settings or device permissions.
- **Usage Information.** Such as the pages or content you view, searches for Listings, bookings you have made, and other actions on the Airbnb Platform.
- **Log Data and Device Information.** Such as details about how you've used the Airbnb Platform (including if you clicked on links to third party applications), IP address, access dates and times, hardware and software information, device information, device event information, unique identifiers, crash data, cookie data, and the pages you've viewed or engaged with before or after using the Airbnb Platform. We may collect this information even if you haven't created an Airbnb account or logged in.
- **Cookies and Similar Technologies as described in our Cookie Policy.**
- **Payment Transaction Information.** Such as payment instrument used, date and time, payment amount, payment instrument expiration date and billing postcode, PayPal email address, IBAN information, your address and other related transaction details.

2.4 Personal Information We Collect from Third Parties.

We collect personal information from other sources, such as:

- **Third-Party Services.** If you link, connect, or login to the Airbnb Platform with a third party service (e.g. Google, Facebook, WeChat), you direct the service to send us information such as your registration, friends list, and profile information as controlled by that service or as authorized by you via your privacy settings at that service.
- **Background Information.** For Members in the United States, to the extent permitted by applicable laws, we may obtain reports from public records of criminal convictions or sex offender registrations. For Members outside of the United States, to the extent permitted by applicable laws and with your consent where required, we may obtain the local version of police, background or registered sex offender checks. We may use your information, including your full name and date of birth, to obtain such reports.
- **Enterprise Product Invitations and Account Management.** Organizations that use our Enterprise products may submit personal information to facilitate account management and invitations to use enterprise products.

- **Referrals and co-travelers.** If you are invited to the Airbnb Platform such as a co-traveler on a trip, the person who invited you can submit personal information about you such as your email address or other contact information.
- **Other Sources.** To the extent permitted by applicable law, we may receive additional information about you, such as [references](#), demographic data or information to help detect fraud and safety issues from third party service providers and/or partners, and combine it with information we have about you. For example, we may receive background check results or fraud warnings from identity verification service providers for use in our fraud prevention and risk assessment efforts. We may receive information about you and your activities on and off the Airbnb Platform, or about your experiences and interactions from our partners. We may receive health information, including but not limited to health information related to contagious diseases.

3. HOW WE USE INFORMATION WE COLLECT

- ⊕ If you reside outside of the United States click [here](#) to learn about our legal bases for collection and processing personal information.

3.1 Provide, Improve, and Develop the Airbnb Platform.

We use personal information to:

- enable you to access the Airbnb Platform and make and receive payments,
- enable you to communicate with other Members,
- perform analytics, debug and conduct research,
- provide customer service,
- send you messages, updates, security alerts, and account notifications,
- if you provide us with your contacts' information such as your friends or co-travellers, we may process this information: (i) to facilitate your referral invitations, (ii) to share your trip details and facilitate trip planning, (iii) for fraud detection and prevention, and (iv) to facilitate your requests or for any other purpose you authorize,
- personalize and customize your experience based on your interactions with the Airbnb Platform, your search and booking history, your profile information and preferences, and other content you submit, and
- enable your use of our enterprise products.

3.2 Create and Maintain a Trusted and Safer Environment.

We use personal information to:

- detect and prevent fraud, spam, abuse, security and safety incidents, and other harmful activity,
- study and combat discrimination consistent with our [Nondiscrimination Policy](#),
- conduct security investigations and risk assessments,
- verify or authenticate information provided by you,
- conduct checks against databases and other information sources, including background or police checks,

- comply with our legal obligations, protect the health and well-being of our Guests, Hosts, Hosts' employees and members of the public,
- resolve disputes with our Members,
- enforce our agreements with third parties,
- comply with law, respond to legal requests, prevent harm and protect our rights (see section 4.5)
- enforce our [Terms](#) and other policies (e.g. [Nondiscrimination Policy](#)), and
- in connection with the activities above, we may conduct profiling based on your interactions with the Airbnb Platform, your profile information and other content you submit to Airbnb, and information obtained from third parties. In limited cases, automated processes could restrict or suspend access to the Airbnb Platform if such processes detect activity that we think poses a safety or other risk to Airbnb, our community, or third parties. If you would like to challenge the decisioning based on the automated process, please contact us via the Contact Information section below.

3.3 Provide, Personalize, Measure, and Improve our Advertising and Marketing. We may use personal information to:

- send you promotional messages, marketing, advertising, and other information based on your preferences and social media advertising through social media platforms,
- personalize, measure, and improve our advertising,
- administer referral programs, rewards, surveys, sweepstakes, contests, or other promotional activities or events sponsored or managed by Airbnb or its third-party partners,
- analyze characteristics and preferences to send you promotional messages, marketing, advertising and other information that we think might be of interest to you, and
- invite you to events and relevant opportunities.

3.4 Provide Payment services. Personal information is used to enable or authorize third parties to use Payment Services:

- Detect and prevent money laundering, fraud, abuse, security incidents.
- Conduct security investigations and risk assessments.
- Comply with legal obligations (such as anti-money laundering regulations).
- Enforce the [Payment Terms](#) and other payment policies.
- With your consent, send you promotional messages, marketing, advertising, and other information that may be of interest to you based on your preferences.
- Provide and improve the Payment Services.

4. SHARING & DISCLOSURE

 If you reside outside of the United States, learn about safeguards we rely on for transferring personal information to recipients outside of the EEA [here](#).

4.1 Sharing With Your Consent or at Your Direction.

Where you provide consent, we share your information as described at the time of consent, such as when authorizing a third-party application or website to access your Airbnb account or participating in promotional activities by Airbnb partners or third parties.

Where permissible with applicable law, we may use certain information about you, such as your email address, de-identify it, and share it with social media platforms, to generate leads, drive traffic to Airbnb or otherwise promote our products and services.

4.2 Sharing Between Members.

To help facilitate bookings or other interactions between Members, we may need to share certain information such as:

- When a booking request is made or dispute is submitted, certain information may be shared between Guest(s) and Host(s), including profile, name, names of any additional Guests, cancellation history, review information, age of guest (unless prohibited by applicable law), dispute outcome (when applicable) and other information you choose to share and submit. When a booking is confirmed, additional information is shared to assist with coordinating the trip, like profile photo and phone number. When you as a Host have a confirmed booking, certain information is shared with the Guest (and the additional Guests they invite, if applicable) to coordinate the booking, such as your profile, full name, phone number, and Listing address.
- When you as a Host invite another Member to host with you, you authorize that person to access and update your information and Member Content, including but not limited to certain information like your full name, phone number, Accommodation address, calendar, Listing information, Listing photos, and email address.
- When you as a Guest invite additional Guests to a booking, your full name, travel dates, Host name, Listing details, the Accommodation address, and other related information will be shared with each additional Guest.

4.3 Information You Publish in Profiles, Listings, and other Public Information.

You can make certain information publicly visible to others, such as:

- Your public profile page, which includes your profile photo, first name, description, and city.
- Listing pages that include information such as the Accommodation or Experience's approximate or precise location description, calendar availability, profile photo, aggregated demand information (like page views over a period of time), and additional information you choose to share.
- Reviews, ratings and other public feedback.
- Content in a community or discussion forum, blog or social media post.

We may display parts of your public profile and other Content you make available to the public like Listing details on third-party sites, platforms and apps.

Information you share publicly on the Airbnb Platform may be indexed through third-party search engines. In some cases, you may opt-out of this feature in your account settings.

4.4 Host Service Providers.

Hosts may use third-party services to help manage or deliver their services, such as cleaning services or lock providers. Hosts may use features on the Airbnb Platform to share information about the Guest (like check-in and check-out dates, Guest name, Guest phone number) with such third-party service providers.

4.5 Complying with Law, Responding to Legal Requests, Preventing Harm and Protecting our Rights.

We may disclose your information to courts, law enforcement, governmental or public authorities, tax authorities, or authorized third parties, if and to the extent we are required or permitted to do so by law or where disclosure is reasonably necessary: (i) to comply with our legal obligations, (ii) to comply with a valid legal request or to respond to claims asserted against Airbnb, (iii) to respond to a valid legal request relating to a criminal investigation to address alleged or suspected illegal activity, or to respond to or address any other activity that may expose us, you, or any other of our users to legal or regulatory liability (more information on Airbnb's Law Enforcement Guidelines [here](#)), (iv) to enforce and administer our [agreements](#) with Members, or (v) to protect the rights, property or personal safety of Airbnb, its employees, its Members, or members of the public. For example, if permitted due to the forgoing circumstances, Host tax information may be shared with tax authorities or other governmental agencies.

Where appropriate, we may notify Members about legal requests unless: (i) providing notice is prohibited by the legal process itself, by court order we receive, or by applicable law, or (ii) we believe that providing notice would be futile, ineffective, create a risk of injury or bodily harm to an individual or group, or create or increase a risk of fraud upon or harm to Airbnb, our Members, or expose Airbnb to a claim of obstruction of justice.

For jurisdictions where Airbnb facilitates the collection and remittance of Taxes where legally permissible according to applicable law, we may disclose Hosts' and Guests' information about transactions, bookings, Accommodations and occupancy Taxes to the applicable tax authority, such as Host and Guest names, Listing addresses, transaction dates and amounts, tax identification number(s), the amount of taxes received (or due) by Hosts from Guests, and contact information.

In jurisdictions where Airbnb facilitates or requires a registration, notification, permit, or license application of a Host with a local governmental authority through Airbnb in accordance with local law, we may share information of participating Hosts with the relevant authority, both during the application process and, periodically thereafter, such as the Host's full name and contact details, Accommodation address, tax identification number, Listing details, and number of nights booked.

4.6 Programs with Managers and Owners.

We may share personal information of Hosts and Guests such as booking information, and information related to compliance with applicable laws such as short-term rental laws with landlords, management companies, and/or property owners (the "**Building Management**"), in order to facilitate programs with Building Management. For example, guest booking and personal information, including guest contact information, may be shared with the Building Management of the building, complex, or community where a host lives and/or the listing is

located, to facilitate hosting services, compliance with applicable laws, security, billing, and other services.

4.7 Host Information Provided to Airbnb for Work Customers.

If a booking is designated as being for business or work purpose and (1) is made by a Guest affiliated with an Enterprise, (2) the Enterprise is enrolled in Airbnb for Work, we may disclose information related to the booking to the Enterprise (e.g., name of the Host, Accommodation address, booking dates, Listing details, etc.) to the extent necessary for the adequate performance of Airbnb's contract with the Enterprise and to provide the services. At the request of the Enterprise or the Guest, we may also share this information with third parties engaged by the Enterprise to provide support services.

4.8 Service Providers.

We share personal information with affiliated and unaffiliated service providers to help us run our business, including service providers that help us: (i) verify your identity or authenticate your identification documents, (ii) check information against public databases, (iii) conduct background or police checks, fraud prevention, and risk assessment, (iv) perform product development, maintenance and debugging, (v) allow the provision of the Airbnb Services through third-party platforms and software tools (e.g. through the integration with our APIs), (vi) provide customer service, advertising, or payments services, (vii) process, handle or assess insurance claims or similar claims, or (viii) facilitate non-profit and charitable activities consistent with Airbnb's mission. These providers are contractually bound to protect your personal information and have access to your personal information to perform these tasks.

4.9 Business Transfers.

If Airbnb undertakes or is involved in any merger, acquisition, reorganization, sale of assets, bankruptcy, or insolvency event, then we may sell, transfer or share some or all of our assets, including your information in connection with such transaction or in contemplation of such transaction (e.g., due diligence). In this event, we will notify you before your personal information is transferred and becomes subject to a different privacy policy.

4.10 Corporate Affiliates.

To support us in providing, integrating, promoting and improving the Airbnb Platform, Payment Services, and our affiliates' services, we may share personal information within our corporate family of companies that are related by common ownership or control. Some examples are:

- **Sharing with Airbnb, Inc.** Even if your country of residence is not the United States, your information will be shared with Airbnb, Inc. which provides the technical infrastructure for the Airbnb Platform.
- **Sharing with Airbnb Payments.** In order to facilitate payments on or through the Airbnb Platform, certain information as described in the "[Outside of the United States](#)" section, will be shared with the relevant Airbnb Payments entity.
- **Sharing with Airbnb Ireland.** Even if your country of residence is the United States, Japan or China, your information may be shared with Airbnb Ireland which provides

customer support and other business operation services to other Airbnb entities.

- **Sharing with Airbnb GSL.** Even if your country of residence is not Japan, your information may be shared with Airbnb GSL which provides customer support and other business operation services to other Airbnb entities.
- **Sharing with Airbnb China.** Even if your country of residence is not China, some of your information will be shared with Airbnb China in the following circumstances:
 - **Public data.** Information you share publicly on the Airbnb Platform.
 - **Creating a Listing.** If you create a Listing in China, information shared includes: (i) your name, phone number, email address, and passport/ID details, (ii) information relating to the Listing (e.g., address), (iii) booking and check-in information relating to the Listing, such as Guest details as set out below in Host Services, dates, time and payment amounts, and (iv) messages between you and prospective and confirmed Guests at the Listing. [Learn more](#)
 - **Host Services.** If you book a Host Service located in China, information shared includes: (i) your name, phone number, and email address (ii) booking and check-in information, including dates and time, (iii) messages between the Host and you or other Guests on the same booking, and (iv) the names, nationalities, gender, date of birth, and passport/ID details of any Guests. [Learn more](#)
 - **Sending Messages.** If you send a message to a Host in relation to that Host's Listing in China, information shared includes your name, profile picture and message content. [Learn more](#)

The data sharing described above is necessary for the performance of the contract between you and us to enable you to list or book Host Services in China and connect with Members in China, and vice versa. Where required under law or if you have expressly granted permission, Airbnb China will disclose your information to Chinese government agencies without further notice to you. We'll notify you in advance in specific situations where we apply any practices that differ from what is described in this Privacy Policy (including practices pertaining to disclosures to government agencies).

5. OTHER IMPORTANT INFORMATION

5.1 Analyzing your Communications.

We may review, scan, or analyze your communications on the Airbnb Platform for reasons outlined in the "How We Use Information We Collect" section of this policy, including fraud prevention, risk assessment, regulatory compliance, investigation, product development, research, analytics, enforcing our [Terms of Service](#), and customer support purposes. For example, as part of our fraud prevention efforts, we scan and analyze messages to mask contact information and references to other sites. In some cases, we may also scan, review, or analyze messages to debug, improve, and expand product offerings. We use automated methods where reasonably possible. Occasionally we may need to manually review communications, such as for fraud investigations and customer support, or to assess and improve the functionality of these automated tools. We will not review, scan, or analyze your messaging communications to send third-party marketing messages to you and we will not sell reviews or analyses of these communications.

5.2 Linking Third-Party Accounts.

You can link your Airbnb account with certain third-party services like social networks. Your contacts on these third-party services are referred to as “Friends.” When you direct the data sharing by creating this link:

- some of the information provided to us from linking accounts may be published on your public profile,
- your activities on the Airbnb Platform may be displayed to your Friends on the Airbnb Platform and/or that third-party service,
- a link to your public profile on that third-party service may be included in your Airbnb public profile,
- other Airbnb users may be able to see any Friends that you may have in common with them, or that you are a Friend of their Friend if applicable,
- other Airbnb users may be able to see any schools, hometowns or other groups you have in common with them as listed on your linked social networking service,
- information you provide to us from the linking of your accounts may be stored, processed and transmitted for fraud prevention and risk assessment purposes, and
- publication and display of information that you provide to the Airbnb Platform through this linkage is subject to your settings and authorizations on the Airbnb Platform and the third-party service.

5.3 Third-Party Partners & Integrations.

Parts of Airbnb may link to third-party services, not owned or controlled by Airbnb, such as Google Maps/Earth. Use of these services is subject to the privacy policies of those providers, such as [Google Maps/Earth Additional Terms of Use](#), [Google Privacy Policy](#) (see [here](#) for more information on how Google uses information), and [Citi Privacy Policy](#). Airbnb does not own or control these third parties and when you interact with them you are providing your information to them.

6. YOUR RIGHTS

You can exercise any of the rights described in this section consistent with applicable law. See [here](#) for information on data subject rights requests and how to submit a request.

Please note that we may ask you to verify your identity and request before taking further action on your request.

 Learn more about rights under GDPR [here](#).

If your country of residence is China, learn more about your rights [here](#).

6.1 Managing Your Information.

You can access and update some of your personal information through your Account settings. If you connected your Airbnb Account to a third-party service, like Facebook or Google, you can change your settings and unlink from that service in your Account settings. You are responsible for keeping your personal information up to date.

6.2 Data Access and Portability.

In some jurisdictions, applicable law may entitle you to request certain copies of your personal information or information about how we handle your personal information, request copies of personal information that you have provided to us in a structured, commonly used, and machine-readable format, and/or request that we transmit this information to another service provider (where technically feasible).

6.3 Data Erasure.

In certain jurisdictions, you can request that your personal information be deleted. Please note that if you request the erasure of your personal information:

- We may retain your personal information as necessary for our legitimate business interests, such as prevention of money laundering, fraud detection and prevention, and enhancing safety. For example, if we suspend an Airbnb Account for fraud or safety reasons, we may retain information from that Airbnb Account to prevent that Member from opening a new Airbnb Account in the future.
- We may retain and use your personal information to the extent necessary to comply with our legal obligations. For example, Airbnb and Airbnb Payments may keep information for tax, legal reporting and auditing obligations.
- Information you have shared with others (e.g., Reviews, forum postings) will continue to be publicly visible on Airbnb, even after your Airbnb Account is cancelled. However, attribution of such information to you will be removed. Some copies of your information (e.g., log records) will remain in our database, but are disassociated from personal identifiers.
- Because we take measures to protect data from accidental or malicious loss and destruction, residual copies of your personal information may not be removed from our backup systems for a limited period of time.

7. SECURITY

While no organization can guarantee perfect security, we are continuously implementing and updating administrative, technical, and physical security measures to help protect your information against unauthorized access, loss, destruction, or alteration.

8. CHANGES TO THIS PRIVACY POLICY

We reserve the right to modify this Privacy Policy at any time in accordance with applicable law. If we do so, we will post the revised Privacy Policy and update the “Last Updated” date at the top. In case of material changes, we will also provide you with notice of the modification by email at least thirty (30) days before the effective date. If you disagree with the revised Privacy Policy, you can cancel your Account. If you do not cancel your Account before the date the revised Privacy Policy becomes effective, your continued access to or use of the Airbnb Platform will be subject to the revised Privacy Policy.

9. CONTACT INFORMATION AND RESPONSIBLE AIRBNB ENTITIES

For questions or complaints about this Privacy Policy or Airbnb’s handling of personal information (i) If you reside in the United States contact Airbnb, Inc., Legal Privacy, 888

Brannan Street, San Francisco, CA 94103 USA; (ii) for payments related matter please use the contact information provided in the [Payments Terms of Service](#) page, and (iii) if you reside outside the United States, please use the contact information for your controller provided in the [Outside of the United States](#) page.

Review the [previous version of this page](#).

Did you get the help you needed?

Yes

No

[Give us feedback](#)

ABOUT

[How Airbnb works](#)

[Newsroom](#)

[Investors](#)

[Airbnb Plus](#)

[Airbnb Luxe](#)

[HotelTonight](#)

[Airbnb for Work](#)

[Made possible by Hosts](#)

[Olympics](#)

[Careers](#)

[Founders' Letter](#)

COMMUNITY

Diversity & Belonging

Against Discrimination

Accessibility

Airbnb Associates

Frontline Stays

Invite friends

Gift cards

Airbnb.org

HOST

Host your home

Host an Online Experience

Host an Experience

Responsible hosting

Resource Center

Community Center

SUPPORT

Our COVID-19 Response

Help Center

Cancellation options

Neighborhood Support

Trust & Safety

 [English \(US\)](#)  [USD](#)

© 2021 Airbnb, Inc. All rights reserved

[Privacy](#) · [Terms](#) · [Sitemap](#)

Boston College Law Review

Volume 56

Issue 6 *Electronic Supplement*

Article 2

5-13-2015

Everybody's Going Surfing: The Third Circuit Approves the Warrantless Use of Internet Tracking Devices in *United States v. Stanley*

Emily W. Andersen

Boston College Law School, emily.andersen@bc.edu

Follow this and additional works at: <http://lawdigitalcommons.bc.edu/bclr>

 Part of the [Constitutional Law Commons](#), [Criminal Law Commons](#), [Fourth Amendment Commons](#), [Internet Law Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

Emily W. Andersen, *Everybody's Going Surfing: The Third Circuit Approves the Warrantless Use of Internet Tracking Devices in United States v. Stanley*, 56 B.C.L. Rev. E. Supp. 1 (2015), <http://lawdigitalcommons.bc.edu/bclr/vol56/iss6/2>

This Comments is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College Law Review by an authorized editor of Digital Commons @ Boston College Law School. For more information, please contact nick.szydlowski@bc.edu.

EVERYBODY'S GOING SURFING: THE THIRD CIRCUIT APPROVES THE WARRANTLESS USE OF INTERNET TRACKING DEVICES IN *UNITED STATES v. STANLEY*

Abstract: On June 11, 2014, in *United States v. Stanley*, the U.S. Court of Appeals for the Third Circuit held that the warrantless use of a tracking device to detect the location of a wireless signal was not a search in violation of the Fourth Amendment. The court reasoned that because the defendant was using his neighbor's open wireless network, the defendant did not have a reasonable expectation of privacy. The court's reasoning was based on a belief that the use of an open wireless network, which is not password protected, is "likely illegal." This comment argues that the Third Circuit erred in refusing to recognize the applicability of the test for "sense-enhancing devices" derived from the 2001 U.S. Supreme Court decision *Kyllo v. United States*. Further, the Third Circuit's holding imperils an activity that many law-abiding citizens engage in daily.

INTRODUCTION

The rapid pace of technological innovation presents a constant challenge for law enforcement, legislatures, and the legal system to keep pace with criminal use of technology.¹ Determined individuals continue to find creative new ways to use technology to engage in criminal activity, while equally determined law enforcement officials seek to thwart them.² Legislators and courts are left to face these innovations as they arise, often without fully understanding the consequences to the general public.³

¹ See, e.g., Matthew Bierlein, *Policing the Wireless World: Access Liability in the Open Wi-Fi Era*, 67 OHIO ST. L. J. 1123, 1125 (2006) (reflecting on the difficulty of applying the law to new technologies while keeping in mind potential ramifications); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 487–88 (2011) (arguing that the Supreme Court's application of the Fourth Amendment evolves as technology changes); Amy E. Wells, *Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet*, 53 OKLA. L. REV. 99, 99 (2000) (arguing that the Internet has made such rapid advances that the law can no longer keep pace).

² See Kerr, *supra* note 1, at 486 (noting that as criminals find new ways to commit crimes, police likewise make use of new methods to solve those crimes). See generally U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, INVESTIGATIONS INVOLVING THE INTERNET AND COMPUTER NETWORKS (2007), available at <https://www.ncjrs.gov/pdffiles1/nij/210798.pdf>, archived at <https://perma.cc/CCA9-EVBX> (identifying various methods of using technology to detect computer and online criminal activity).

³ See Anne Meredith Fulton, *Cyberspace and the Internet: Who Will Be the Privacy Police?*, 3 COMMLAW CONSPPECTUS 63, 70 (1995) (stating that legislators cannot fashion adequate laws

In June 2014, in *United States v. Stanley*, the U.S. Court of Appeals for the Third Circuit faced a question regarding the legality of tracking technology used by the Pennsylvania State Police.⁴ Law enforcement used this technology to locate the defendant, Richard Stanley, who was suspected of transmitting child pornography by “mooching” off of his neighbor’s unprotected wireless Internet signal.⁵ The technology traced the source of the defendant’s wireless signal using an antenna and software called “Moocherhunter™.”⁶ The Third Circuit held that use of this technology by the police, which located Stanley while he was using his computer within his home, was not an unlawful search.⁷ The Third Circuit, therefore, affirmed the lower court’s ruling that a warrant was not required to use the technology.⁸

until they understand the technology they are regulating); Eli R. Shindelman, *Time for the Court to Become “Intimate” with Surveillance Technology*, 52 B.C. L. REV. 1909, 1911 (2011) (arguing that surveillance technology has advanced faster than Fourth Amendment jurisprudence).

⁴ See *United States v. Stanley (Stanley II)*, 753 F.3d 114, 115–16 (3d Cir. 2014) (describing the technology), cert. denied, 135 S. Ct. 507 (2014).

⁵ See *id.* at 116–17.

⁶ *Id.* at 116. Mirroring the Third Circuit’s opinion, future references to Moocherhunter encompass the software as well as the computer and directional antenna that are used with the software. *See id.* at 116 n.5.

⁷ *See id.* at 115.

⁸ *See id.* Other circuits have not yet ruled on whether a warrant is required before using similar technology to locate individuals suspected of computer and/or Internet crimes. *See Response Brief for the United States at 41*, *Stanley II*, 753 F.3d 114 (No. 13-1910), 2013 WL 5427843, at *41. District courts have applied the third party doctrine from *Smith v. Maryland*, 442 U.S. 735 (1979), to the same or similar technology. *See Stanley II*, 753 F.3d at 122. In 2013, in *United States v. Norris*, the U.S. District Court for the Eastern District of California cited the lower court’s opinion in *Stanley* and found that use of the same technology, Moocherhunter, to locate the defendant did not require a warrant. *See No. 2:11-cr-00188-KJM*, 2013 WL 4737197, at *8 (E.D. Cal. Sept. 3, 2013). The court reached that decision by applying the third party doctrine. *See id.* In 2012, in *United States v. Broadhurst*, the U.S. District Court for the District of Oregon found that evidence obtained after police used similar technology to locate defendant and obtain a search warrant was not admissible because police trespassed on defendant’s property in order to use the technology. *See No. 3:11-cr-00121-MO-1*, 2012 WL 5985615, at *6 (D. Or. Nov. 28, 2012). Apart from police error, the court applied the third party doctrine and found that use of the technology would not have required a warrant. *See id.* at *4.

C. United States v. Stanley in the District Court

In November 2010, the routine investigations of the Pennsylvania State Police led to the discovery of a computer sharing child pornography through a peer-to-peer file-sharing network.⁴⁰ After tracing the activity to Stanley's neighbor's router, law enforcement obtained a search warrant and performed a search of the neighbor's home.⁴¹ Law enforcement found two computers in the neighbor's home, though neither contained the files in question.⁴² Law enforcement also found a wireless router in the home.⁴³ Stanley's neighbor had not password-protected his router, leading law enforcement to infer that a third computer within range of the router had accessed it from outside the neighbor's home.⁴⁴ Law enforcement located the third computer and the like-

⁴⁰ See *United States v. Stanley (Stanley I)*, No. 11–272, 2012 WL 5512987, at *2–3 (W.D. Pa. Nov. 14, 2012), *aff'd*, 753 F.3d 114 (3d Cir. 2014). Law enforcement discovered the file-sharing user's public IP address and identified it as a Comcast IP address. *Id.* Police then obtained a court order to compel Comcast to share information regarding the name and address of the subscriber with that public IP address. *Id.* This led police to Stanley's neighbor, the Comcast subscriber. *Id.*

⁴¹ See *id.* at *3.

⁴² *Id.*

⁴³ See *id.* Wireless routers assign unique IP addresses to each computer that accesses the Internet through the router. *Id.* at *4. Upon inspection of the neighbor's wireless router, law enforcement discovered that the router had assigned three unique IP addresses, yet the neighbor's computers used only two of those numbers. See *id.* at *5. Law enforcement determined that their suspect must have been assigned the third unique IP address associated with the router. *See id.*

⁴⁴ See *Stanley II*, 753 F.3d at 115–16. The neighbor confirmed that he had not given anyone explicit permission to access his router. See *Stanley I*, 2012 WL 5512987, at *3. Wireless routers typically transmit and receive radio signals from a radius of 300 feet. Reply Brief for Appellant at 24, *Stanley II*, 753 F.3d 114 (No. 13-1910), 2013 WL 5869880, at *24. Law enforcement searched the settings on the wireless router and identified the MAC address of the computer (a unique number) associated with the third IP address, yet law enforcement was unable to locate the computer with this information alone. See *Stanley I*, 2012 WL 5512987, at *5–6; see also *Broadhurst*, 2012 WL 5985615, at *6 (noting that the defendant's wireless signal could have been transmitted to the router in question from anywhere, making use of tracking technology necessary to locate the defendant). Law enforcement was, however, able to confirm that the third computer had accessed the file-sharing network. See *Stanley II*, 753 F.3d at 117; *Stanley I*, 2012 WL 5512987, at *5–6.

ly suspect by using tracking technology available to the Pennsylvania State Police—Moocherhunter.⁴⁵

Moocherhunter tracks the location of unauthorized wireless users, or “moochers,” by utilizing a directional antenna to trace a computer or device transmitting signals to and from a wireless router.⁴⁶ Using Moocherhunter, law enforcement tracked the unauthorized user by following the signal the third computer was transmitting to and from the router.⁴⁷ The signal was strongest when law enforcement stood on the sidewalk outside of Stanley’s apartment door.⁴⁸

After identifying Stanley’s address, law enforcement was able to obtain a search warrant.⁴⁹ During the search of his apartment, Stanley confessed to using his neighbor’s wireless signal to access child pornography.⁵⁰ Stanley was indicted on one count of possession of child pornography under 18 U.S.C. § 2252(a)(4)(B).⁵¹ Stanley pled not guilty to the charge and filed a motion to suppress evidence gathered by police and statements he made during the search.⁵² Stanley argued that law enforcement’s use of Moocherhunter to locate his laptop computer within his home constituted a search that required a warrant.⁵³ On November 14, 2012, the U.S. District Court for the Western District of Pennsylvania denied Stanley’s motion.⁵⁴ Stanley then appealed to the U.S. Court of Appeals for the Third Circuit, which affirmed the lower court’s decision on June 11, 2014.⁵⁵ The Third Circuit held that Stanley did not have a “legitimate” expectation of privacy in transmitting child pornography through his neighbor’s wireless router.⁵⁶ The U.S. Supreme Court denied Stanley’s petition for writ of certiorari on November 10, 2014.⁵⁷

⁴⁵ See *Stanley I*, 2012 WL 5512987, at *7–8. Pennsylvania State Police were unsure as to whether or not use of the software required a search warrant, and called the U.S. Attorney’s Office for advice. See *id.* at *6. Based on that conversation, law enforcement decided a search warrant was unnecessary. See *Stanley II*, 753 F.3d at 117.

⁴⁶ *Stanley I*, 2012 WL 5512987, at *6. Pennsylvania State Police used Moocherhunter in “passive mode” in order to locate Stanley’s computer. *Id.* Moocherhunter can also be used in “active mode” in order to trace any wireless signal transmitted to any wireless router. *Id.*

⁴⁷ See *id.* at *7–8. Law enforcement entered the MAC address for the suspect’s computer into the police-owned laptop with Moocherhunter installed and attached a directional antenna to track the signal. See *id.* at *7.

⁴⁸ See *id.* at *8.

⁴⁹ See *id.*

⁵⁰ *Stanley II*, 753 F.3d at 117. Law enforcement found 144 files containing images and videos of child pornography on Stanley’s laptop computer. *Id.*

⁵¹ 18 U.S.C. § 2252(a)(4)(B) (2012); *Stanley I*, 2012 WL 5512987, at *1.

⁵² *Stanley I*, 2012 WL 5512987, at *1.

⁵³ See *Stanley II*, 753 F.3d at 119.

⁵⁴ *Stanley I*, 2012 WL 5512987, at *22.

⁵⁵ *Stanley II*, 753 F.3d at 114–15.

⁵⁶ See *id.* at 124.

⁵⁷ See *Stanley v. United States*, 135 S. Ct. 507 (2014) (denying petition for writ of certiorari).

II. THE THIRD CIRCUIT SEEKS LEGITIMACY IN REASONABLE EXPECTATIONS OF PRIVACY

On appeal, the U.S. Court of Appeals for the Third Circuit affirmed the U.S. District Court for the Western District of Pennsylvania's finding while clarifying the district court's reasoning.⁵⁸ The Third Circuit agreed that the expectation of privacy test was appropriate but rejected the district court's application of the third party doctrine to the facts of the case.⁵⁹ This Part reviews the Third Circuit's holding, beginning with its rejection of the third party doctrine.⁶⁰ This Part then reviews the Third Circuit's application of the expectation of privacy test.⁶¹ Lastly, this Part discusses why the Third Circuit rejected the test developed in *Kyllo v. United States*.⁶²

The Third Circuit rejected the lower court's application of the third party doctrine.⁶³ The district court found that because Stanley transmitted information to his neighbor's router, Stanley had assumed the risk of that information being given to police.⁶⁴ The Third Circuit held that this application of the third party doctrine was too broad, as all Internet traffic requires sharing information with third parties, such as servers.⁶⁵ Because the information transmitted to these third parties includes much beyond the basic data of telephone numbers dialed from a home telephone, the Third Circuit feared

⁵⁸ See *United States v. Stanley (Stanley II)*, 753 F.3d 114, 124 (3d Cir. 2014), cert. denied, 135 S. Ct. 507 (2014).

⁵⁹ See *id.* at 122.

⁶⁰ See *infra* notes 63–66 and accompanying text.

⁶¹ See *infra* notes 67–70 and accompanying text.

⁶² See *infra* notes 71–74 and accompanying text.

⁶³ See *Stanley II*, 753 F.3d at 122; *supra* notes 30–32 and accompanying text (discussing the third party doctrine). The Third Circuit's holding is also counter to the lower court findings in *United States v. Norris* and *United States v. Broadhurst*. See *Stanley II*, 753 F.3d at 122; *United States v. Norris*, No. 2:11-cr-00188-KJM, 2013 WL 4737197, at *8 (E.D. Cal. Sept. 3, 2013) (holding that defendant did not have a reasonable expectation of privacy in Internet data transmitted to a third party); *United States v. Broadhurst*, No. 3:11-cr-00121-MO-1, 2012 WL 5985615, at *5 (D. Or. Nov. 28, 2012) (holding that defendant did not have a reasonable expectation of privacy because he transmitted information to a third party).

⁶⁴ See *United States v. Stanley (Stanley I)*, No. 11-272, 2012 WL 5512987, at *12 (W.D. Pa. Nov. 14, 2012), *aff'd*, 753 F.3d 114 (3d Cir. 2014). The Third Circuit corrected the technological leap made by the lower court regarding exactly what Stanley transmitted to a third party. See *Stanley II*, 753 F.3d at 123–24. The lower court seemed to suggest that Stanley had transmitted his physical address to his neighbor's router, which the neighbor was then able to give to police. See *id.* Instead, police were only able to obtain discrete data from the neighbor's router—Stanley's IP and MAC addresses—that police then input into Moocherhunter to locate Stanley. See *id.*

⁶⁵ See *Stanley II*, 753 F.3d at 124; Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 585 (2011) (noting that third parties like Internet Service Providers and websites have access to a broad range of data transmitted by Internet users).

providing law enforcement with “unfettered access” to individuals’ Internet data without adequate Fourth Amendment protection.⁶⁶

After eliminating the third party doctrine from its analysis, the Third Circuit applied the expectation of privacy test and held that Stanley did not have a reasonable expectation of privacy because of the “dubious legality” of using his neighbor’s wireless signal.⁶⁷ In so holding, the Third Circuit relied on a piece of analysis that the U.S. Supreme Court added to the expectation of privacy test.⁶⁸ In 1978, in *Rakas v. Illinois*, the U.S. Supreme Court added a requirement that a reasonable expectation of privacy must also be “legitimate,” or lawful.⁶⁹ Therefore, in addition to Stanley’s mode of access to the Internet, the Third Circuit held that given the illegality of Stanley’s transmission of child pornography, society would not recognize Stanley’s expectation of privacy as reasonable.⁷⁰

Finally, the Third Circuit held that the test set out in *Kyllo* was inadequate given Stanley’s use of a “virtual arm” to extend his activities outside of his home.⁷¹ The Third Circuit addressed the similarities between law enforcement’s use of Moocherhunter and law enforcement’s use of a thermal

⁶⁶ See *Smith v. Maryland*, 442 U.S. 735, 743 (1979) (holding that customers do not have an expectation of privacy in telephone numbers dialed from their home telephone); *Stanley II*, 753 F.3d at 124 (indicating reluctance to apply the third party doctrine to all signals sent to third parties).

⁶⁷ See *Stanley II*, 753 F.3d at 120–22 (reviewing case law to arrive at the conclusion that Stanley lacked a reasonable expectation of privacy); *supra* notes 28–29 and accompanying text (discussing the expectation of privacy test). Under the expectation of privacy test, in order to enjoy Fourth Amendment protection, an expectation of privacy must be both subjectively and objectively reasonable. See *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The Third Circuit held that although Stanley may have had a subjective expectation of privacy, he did not have an objective expectation of privacy because of his “likely illegal” use of his neighbor’s router. *See Stanley II*, 753 F.3d at 120–22.

⁶⁸ See *Stanley II*, 753 F.3d at 120–22. This addition was explained in 1978, in *Rakas v. Illinois*, when the U.S. Supreme Court stated that the reasonable expectation of privacy inquiry is necessarily negated when society would view the activity in question as “wrongful.” 439 U.S. 128, 143–44 n.12 (1978) (quoting *United States v. Jones*, 362 U.S. 257, 267 (1960)) (internal quotations omitted).

⁶⁹ 439 U.S. at 143–44 n.12; *see Stanley II*, 753 F.3d at 120–22. The Third Circuit, citing to a footnote in *Rakas*, compared Stanley’s expectation of privacy to a burglar’s unreasonable expectation of privacy while stealing items from an unoccupied summerhouse. *Stanley II*, 753 F.3d at 120 (citing *Rakas*, 439 U.S. at 143–44 n.12). The Court described Stanley as a “virtual trespasser” who had “hijacked” his neighbor’s wireless router. *Id.* The Third Circuit noted that Pennsylvania, like several other states, has statutes that might possibly apply to wireless mooching. *See* 18 PA. CONS. STAT. §§ 3926 (“Theft of services”), 7611 (“Unlawful use of computer and other computer crimes”) (2014); *Stanley II*, 753 F.3d at 120–21 nn.10–11.

⁷⁰ *See Stanley II*, 753 F.3d at 121, 124.

⁷¹ *See id.* at 119–20; *supra* notes 36–39 and accompanying text (discussing the holding in *Kyllo*). In 2001, in *Kyllo v. United States*, the U.S. Supreme Court held that a warrant is required for devices that can sense activity within the home that would not be detectable without entering the home. *See* 533 U.S. 27, 40 (2001).

sensor to scan the interior temperature of a home in *Kyllo*.⁷² Although the Third Circuit acknowledged that Moocherhunter met the requirements of the *Kyllo* test for sense-enhancing devices, the court stated that *Kyllo* only applies to activities that are confined within the home.⁷³ Because Stanley sent data outside of his home to his neighbor's router, the Third Circuit held that his actions were removed from the "safe harbor" of *Kyllo*, defeating the objective prong of the expectation of privacy test.⁷⁴

⁷² See *Kyllo*, 533 U.S. at 40; *Stanley II*, 753 F.3d at 119.

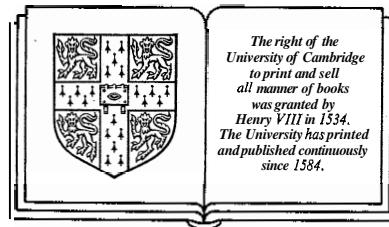
⁷³ See *Kyllo*, 533 U.S. at 40; *Stanley II*, 753 F.3d at 119. Moocherhunter was held to be sense-enhancing technology that is not in general use and can gather information about activity within the home that, absent use of the technology, could not be obtained without entering the home. See *Kyllo*, 533 U.S. at 34; *Stanley II*, 753 F.3d at 119.

⁷⁴ See *Stanley II*, 753 F.3d at 120. The court acknowledged that Moocherhunter met the requirements for sense-enhancing devices that require a warrant. See *id.* at 119. The Third Circuit distinguished the facts in *Kyllo* by stating that the defendant in *Kyllo* had confined his activities within the home. See *Kyllo*, 533 U.S. at 34; *Stanley II*, 753 F.3d at 119. The Third Circuit held that *Kyllo* did not apply because Stanley transmitted data outside of his home. See *Stanley II*, 753 F.3d at 119–20. In addition, in *Kyllo*, the Supreme Court was particularly concerned with the fact that the thermal sensor police used could detect any activity, legal or illegal, taking place within the home. See *Illinois v. Caballes*, 543 U.S. 405, 409–10 (2005) ("Critical to that decision [in *Kyllo*] was the fact that the *device was capable of detecting lawful activity*—in that case, intimate details in a home, such as 'at what hour each night the lady of the house takes her daily sauna and bath.'" (citing *Kyllo*, 533 U.S. at 38) (emphasis added)); 533 U.S. at 38. The Third Circuit focused only on the possible illegality of Stanley's actions. See *Stanley II*, 753 F.3d at 119–20. The Third Circuit determined that Stanley lacked a "legitimate" expectation of privacy when engaging in the "likely illegal" activity of accessing an unprotected wireless signal. See *id.*

*Philosophical Dimensions
of Privacy:
An Anthology*

Edited by
FERDINAND DAVID SCHOEMAN
*Department of Philosophy
University of South Carolina, Columbia*

© Cambridge University Press 1984



CAMBRIDGE UNIVERSITY PRESS

CAMBRIDGE
LONDON NEW YORK NEW ROCHELLE
MELBOURNE SYDNEY

Privacy as an aspect of human dignity

An Answer to Dean Prosser

EDWARD J. BLOUSTEIN

I. Introduction

Three-quarters of a century have passed since Warren and **Brandes** published their germinal article, "The Right of Privacy."¹ In this period many hundreds of cases, ostensibly founded upon the right to privacy, have been decided,* a number of statutes expressly embodying it have been enacted,³ and a sizeable scholarly literature has been devoted to it.⁴ Remarkably enough, however, there remains to this day considerable confusion concerning the nature of the interest which the right to privacy is designed to protect. The confusion is such that in 1956 a distinguished federal judge characterized the state of the law of privacy by likening it to a "haystack in a hurricane."⁵ And, in 1960, the dean of tort scholars wrote a comprehensive article on the subject which, in, effect, repudiates Warren and **Brandes** by suggesting that privacy is not an independent value at all but rather a composite of the interests in reputation, emotional tranquility and intangible property.⁶

My purpose in this article is to propose a general theory of individual privacy which will reconcile the divergent strands of legal development—which will put the straws back into the haystack. The need for such a theory is pressing. In the first place, the disorder in the cases and **commentary offends** the primary canon of all science that a single general principle of explanation is to be preferred over a congeries of discrete rules. Secondly, the conceptual disarray has had untoward effects on the courts; lacking a clear sense of what interest or interests are involved in privacy cases has made it difficult to arrive at a judicial consensus concerning the elements of the wrong or the nature of the defenses to it. Thirdly, analysis of the interest

involved in the privacy cases is of utmost significance because in our own day scientific and technological advances have raised the spectre of new and frightening invasions of privacy.⁷ Our capacity as a society to deal with the impact of this new technology depends, in part, on the degree to which we can assimilate the threat it poses to the settled ways our legal institutions have developed for dealing with similar threats in the past.

The concept of privacy has, of course, psychological, social and political dimensions which reach far beyond its analysis in the legal context;⁸ I will not deal with these, however, except incidentally. Nor do I pretend to give anything like a detailed exposition of the requirements for relief and the character of the available defenses in the law of privacy. Nor will my analysis touch on privacy problems of organizations and groups. My aim is rather the more limited one of discovering in the welter of cases and statutes the interest or social value which is sought to be vindicated in the name of individual privacy.

I propose to accomplish this by examining in some detail Dean Prosser's analysis of the tort of privacy and by then suggesting the conceptual link between the tort and the other legal contexts in which privacy finds protection. My reasons for taking this route rather than another, for concentrating initially on the tort cases and Dean Prosser's analysis of them, are that privacy began its modern history as a tort and that Dean Prosser is by far the most influential contemporary exponent of the tort. Warren and **Brandes** who are credited with "discovering" privacy thought of it almost exclusively as a tort remedy. However limited and inadequate we may ultimately consider such a remedy, the historical development in the courts of the concept of privacy stems from and is almost exclusively devoted to the quest for such a civil remedy. We neglect it, therefore, only at the expense of forsaking the valuable insights which seventy-five years of piecemeal common law adjudication can provide.

The justification for turning my own search for the meaning of privacy around a detailed examination of Dean Prosser's views on the subject is simply that his influence on the development of the law of privacy begins to rival in our day that of Warren and **Brandes**.⁹ His concept of privacy is alluded to in almost every decided privacy case in the last ten years or so,¹⁰ and it is reflected in the current draft of the Restatement of Torts.¹¹ Under these circumstances, if he is mistaken, as I believe he is, it is obviously important to attempt to demonstrate his error and to attempt to provide an alternative theory.

II. Dean Prosser's analysis of the privacy cases

Although it is not written in the style of an academic exposé of a legal myth, Dean Prosser's 1960 article on privacy has that effect; although he does not say it in so many words, the clear consequence of his view is that Warren and Brandeis were wrong, and their analysis of the tort of privacy a mistake. For, after examining the "over three hundred cases in the books,"¹² in which a remedy has ostensibly been sought for the same wrongful invasion of privacy, he concludes that, in reality, what is involved "is not one tort, but a complex of four."¹³ A still more surprising conclusion is that these four torts involve violations of "four different interests,"¹⁴ none of which, it turns out, is a distinctive interest in privacy.¹⁵

The "four distinct torts" which are discovered in the cases are described by Dean Prosser as follows:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing facts about the plaintiff.
3. Publicity which places the plaintiff in a "false light" in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.¹⁶

The interest protected by each of these torts is: in the intrusion cases, the interest in freedom from mental distress,¹⁷ in the public disclosure and "false light" cases, the interest in reputation,¹⁸ and in the appropriation cases, the proprietary interest in name and likeness.¹⁹

Thus, under Dean Prosser's analysis, the much vaunted and discussed right to privacy is reduced to a mere shell of what it has pretended to be. Instead of a relatively new, basic and independent legal right protecting a unique, fundamental and relatively neglected interest, we find a mere application in novel circumstances of traditional legal rights designed to protect well-identified and established social values. Assaults on privacy are transmuted into a species of defamation, infliction of mental distress and misappropriation. If Dean Prosser is correct, there is no "new tort" of invasion of privacy, there are rather only new ways of committing "old torts." And, if he is right, the social value or interest we call privacy is not an independent one, but is only a composite of the value our society places on protecting mental tranquility, reputation and intangible forms of property.

III. Dean Prosser's analysis appraised

A. Consistency with the Warren and Brandeis analysis

One way of testing Dean Prosser's analysis and of illuminating the concept of privacy itself, is to compare it with the Warren-Brandeis article.²⁰ Did those learned authors propose a "new tort" or merely a new name for "old torts"?

We may begin by noting the circumstances which stimulated the writing of the article. "On January 25, 1883," Brandeis biographer writes,

Warren had married Miss Mabel Bayard, daughter of Senator Thomas Francis Bayard, Sr. They set up housekeeping in Boston's exclusive Back Bay section and began to entertain elaborately. The Saturday *Evening Gazette*, which specialized in "blue blood items" naturally reported their activities in lurid detail. This annoyed Warren who took the matter up with Brandeis. The article was the result.²¹

The article itself presents an intellectualized and generalized account of the plight of the Warrens beleaguered by the yellow journalism of their day.

Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good 'the prediction that "what is whispered in the closet shall be proclaimed from the house tops."²²

The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle.²³

Thus, Warren and Brandeis were disturbed by lurid newspaper gossip concerning private lives. But what, in their view, made such gossip wrongful? What value or interest did such gossip violate to give it a tortious character? How, in other words, were people hurt by such gossip?

On more than one occasion in their article, they allude to the "distress" which "idle gossip" in newspapers causes. "[M]odern enterprise and invention," they write, "have, through invasions . . . [of man's] privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."²⁴ And they mention "the

suffering of those who may be made the subjects of journalistic or other enterprise.”²⁵

These allusions to mental distress seem to afford support for Dean Prosser’s view that, in one of its aspects, at least, the right to privacy protects against intentionally inflicted emotional trauma; that the gravaman of an action for the invasion of privacy is really hurt feelings.²⁶ Such a conclusion, however, cannot be justified by the Warren and Brandeis article because, in fact, they expressly disown it. They point out that, although “a legal remedy for . . . [invasion of privacy] seems to involve the treatment of mere wounded feelings,”²⁷ the law affords no remedy for “mere injury to feelings. However painful the mental effects upon another of an act, though purely wanton or even malicious, yet if the act is otherwise lawful the suffering inflicted is without legal remedy.”²⁸ And they then go on to distinguish invasion of privacy as “a legal *injuria*” or “act wrongful in itself” from “mental suffering” as a mere element of damages.²⁹

Thus, in Warren and Brandeis’ view, idle gossip about private affairs may well cause mental distress, but this is not what makes it wrongful; the mental distress is, for them, parasitic of an independent tort, the invasion of privacy. Nor did they believe, as evidently Dean Prosser believes, that “public disclosure of private facts” constitutes a species of defamation and an injury to reputation.³⁰

“The principle on which the law of defamation rests,” they say, “covers . . . a radically different class of effects from those for which attention is now asked.”³¹ Defamation concerns “injury done to the individual in his external relations to the community,” injury to the estimation in which others hold him; the wrong involved in defamation is “material.”³² The invasion of privacy, by contrast, involves a “spiritual” wrong, an injury to a man’s “estimate of himself” and an assault upon “his own feelings.”³³ Moreover, invasion of privacy does not rest upon falsity as does defamation; the right to privacy exists not only “to prevent inaccurate portrayal of private life, but to prevent its being depicted at all.”³⁴

The third interest or value which Warren and Brandeis examine as the possible basis of the wrongfulness of newspaper gossip concerning private lives is a proprietary or property interest. Here as well, their conclusion is the negative one that, although the invasion of privacy may involve, on occasion, a misappropriation of something of pecuniary value, this is not the essence of the wrong.

This conclusion is the more striking because the legal precedents upon which they rely for the erection of a right to privacy are cases enforcing so-called common law property rights in literary and artistic

works and cases involving trade secrets.³⁵ It is also a strong argument against Dean Prosser’s identification of a “distinct” tort of appropriation of name or likeness as involving the protection of a proprietary interest³⁶ because, although they primarily concentrate on publicity cases, they expressly take account of the cases involving an unconsented use of a photographic likeness.³⁷

Warren and Brandeis announce at the outset of their article that they believe that “the legal doctrines relating to infraction of what is ordinarily termed the common-law right to *intellectual and artistic property*” can, “properly understood,” provide “a remedy for the evils under consideration.”³⁸ They distinguish, however, between the common law protection of such property and that secured by forms of copyright statutes. The common law right allows a man “to control absolutely the act of publication, and in the exercise of his own discretion, to decide whether there shall be any publication at all.”³⁹ The statutory right, by contrast, aims “to secure to the author, composer or artist the entire profits arising from publication.”⁴⁰

This distinction between the purposes of common law and statutory protection of literary and artistic property provides, in the Warren and Brandeis analysis, a key to the underlying significance of common law rights to literary and artistic property. They are really nothing but “instances and applications of a general right to privacy”⁴¹ because “the value of the production [of a work subject to common law property right] is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all.”⁴² This being so, “it is difficult to regard the [common law] right as one of property.”⁴³

It is admitted that the courts which erected the legal remedy which “secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others,”⁴⁴ had, for the most part, “asserted that they rested their decisions on the narrow grounds of protection of property.”⁴⁵ Yet, according to Warren and Brandeis, no thing of pecuniary value, no right of property “in the narrow sense,” is to be found at issue in many of the cases. The concept of “property” was put forward by the courts as a fiction to rationalize a form of legal relief which was really founded on other grounds of policy. In other words, what we mean by saying there is common law property in literary and artistic works is not that violation of the right involves destruction or appropriation of something of monetary value but rather only that the law affords a remedy for the violation.⁴⁶

In sum, as far as Warren and Brandeis were concerned, newspaper

gossip about private lives was not a wrong because it destroyed character, caused mental distress, or constituted a misappropriation of property—a taking of something of pecuniary value. Although the yellow journalism which feeds luridly upon the details of private lives may incidentally accomplish each of these results, they are not the essence of the wrong. Mrs. Warren's reputation could have been completely unaffected, her equanimity entirely unruffled, and her fortune wholly undisturbed; the publicity about her and her husband would nevertheless be wrongful, nevertheless be in violation of an interest which the law should protect.

What then is the basis of the wrong? Unfortunately, the learned authors were not as successful in describing the interest violated by publicity concerning private lives as in saying what it was not. This explains, in part, the fact that after hundreds of cases enforcing Warren and Brandeis' "right to privacy," Dean Prosser, Harper and James,⁴⁷ the Restatement of Torts,⁴⁸ and other learned authorities⁴⁹ predicate the right on bases expressly rejected by Warren and Brandeis.

Warren and Brandeis obviously felt that the term "privacy" was in itself a completely adequate description of the interest threatened by an untrammeled press; man, they said, had a right to his privacy, a right to be let alone, and this was, for them, a sufficient description of the interest with which they were concerned. This right, although violated by publication of information about a person's life and character, much in the same way the right to reputation is violated, is not the same as the right to reputation. Nor is the interest in being let alone like that of being protected against attempts to inflict mental trauma, even though distress is the frequent accompaniment of intrusions on privacy. And, although the common law property right to literary and artistic products is an instance of the right to privacy, privacy is not to be confused with something of pecuniary value.

Warren and Brandeis went very little beyond thus giving "their right" and "their interest" a name and distinguishing it from other rights or interests. It is only in asides of characterization and passing attempts at finding a verbal equivalent of the principle of privacy that we may find any further clues to the interest or value they sought to protect. Thus, at one point they remark, as I have indicated above, that, unlike reputation which is a "material" value, privacy is a "spiritual" one.⁵⁰ And they make repeated suggestions that the invasion of privacy, in some way, involves man's mentality,⁵¹ that it involves an "effect upon . . . [a man's] estimate of himself and upon his own feeling ~ . " ~ ~

The most significant indication of the interest they sought to protect,

however, is in their statement that "the principle which protects personal writings and all other personal productions . . . against publication in any form is in reality not the principle of private property, but that of *inviolate personality*."⁵² I take the principle of "inviolate personality" to posit the individual's independence, dignity and integrity; it defines man's essence as a unique and self-determining being. It is because our Western ethico-religious tradition posits such dignity and independence of will in the individual that the common law secures to a man "literary and artistic property"—the right to determine "to what extent his thoughts, sentiments, emotions shall be communicated to others."⁵³ The literary and artistic property cases led Warren and Brandeis to the concept of privacy because, for them, it would have been inconsistent with a belief in man's individual dignity and worth to refuse him the right to determine whether his artistic and literary efforts should be published to the world. He would be less of a man, less of a master over his own destiny, were he without this right.

Thus, I believe that what provoked Warren and Brandeis to write their article was a fear that a rampant press feeding on the stuff of private life would destroy individual dignity and integrity and emasculate individual freedom and independence. If this is so, Dean Prosser's analysis of privacy stands clearly at odds with "the most influential law review article ever published," one which gave rise to a "new tort,"⁵⁴ not merely to a fancy name for "old torts."

As I have already indicated,⁵⁵ Dean Prosser's analysis of the privacy cases is remarkable for two propositions; the first, that there is not a single tort of the invasion of privacy, but rather "four distinct torts"; the second, that there is no distinctive single value or interest which these "distinct torts" protect and that, in fact, they protect three different interests, no one of which can properly be denominated an interest in privacy. I have considerable doubt that the cases support either of these conclusions.

B. The intrusion cases

This category of cases comprises instances in which a defendant has used illegal or unreasonable means to discover something about the plaintiff's private life.⁵⁶ Included in the category, thus, is a case in which a defendant was an unwanted spectator to the plaintiff giving birth to her child.⁵⁷ The Michigan court, writing nine years before Warren and Brandeis, declared the wrong was actionable in tort because "to the plaintiff the occasion was a most sacred one and no one

had a right to intrude unless invited or because of some real and pressing necessity."⁵⁹

Another illustrative case is *Rhodes v. Graham*,⁶⁰ where the defendant tapped the plaintiff's telephone wires without authorization. In upholding the cause of action for damages the court declared that "the evil incident to the invasion of the privacy of the telephone is as great as that accompanied by unwarranted publicity in newspapers and by other means of a man's private affairs."⁶¹ In still another case of the same type, where a home was illegally entered, a cause of action for damages was upheld on the theory of a violation of state constitutional search and seizure provisions.⁶²

What interest or value is protected in these cases? Dean Prosser's answer is that "the gist of the wrong [in the intrusion cases] is clearly the intentional infliction of mental distress."⁶³

The fact is, however, that in no case in this group is mental distress said by the court to be the basis or gravamen of the cause of action. Moreover, all but one of these decisions predate the recognition in the jurisdictions concerned of a cause of action for intentionally inflicted mental distress⁶⁴ and, in most instances, the lines of authority relied upon in the intrusion cases are quite different from those relied upon in the mental distress cases.⁶⁵

Furthermore, special damages in the form of "severe emotional distress" is recognized by Dean Prosser⁶⁶ and other authorities⁶⁷ as a requisite element of the cause of action for intentionally inflicted emotional distress. Yet, many of the cases allowing recovery for an intrusion expressly hold that special damages are not required.⁶⁸ Except in a small number of the cases of this group, there does not even seem to have been an allegation of mental illness or distress, certainly not an allegation of serious mental illness. And even in one of the rare cases in which serious mental distress was alleged, the court expressly says that recovery would be available without such an allegation.⁶⁹

The most important reason, however, for disputing Dean Prosser's thesis in regard to the intrusion cases is that, in my judgment, he neglects the real nature of the complaint; namely that the intrusion is demeaning to individuality, is an affront to personal dignity. A woman's legal right to bear children without unwanted onlookers does not turn on the desire to protect her emotional equanimity, but rather on a desire to enhance her individuality and human dignity. When the right is violated she suffers outrage or affront, not necessarily mental trauma or distress. And, even where she does undergo anxiety or other symptoms of mental illness as a result, these consequences themselves flow from the indignity which has been done to her.

The fundamental fact is that our Western culture defines individuality as including the right to be free from certain types of intrusions. This measure of personal isolation and personal control over the conditions of its abandonment is of the very essence of personal freedom and dignity, is part of what our culture means by these concepts. A man whose home may be entered at the will of another, whose conversation may be overheard at the will of another, whose marital and familial intimacies may be overseen at the will of another, is less of a man, has less human dignity, on that account. He who may intrude upon another at will is the master of the other and, in fact, intrusion is a primary weapon of the tyrant.⁷⁰

I contend that the gist of the wrong in the intrusion cases is not the intentional infliction of mental distress but rather a blow to human dignity, an assault on human personality. Eavesdropping and wire-tapping, unwanted entry into another's home, may be the occasion and cause of distress and embarrassment but that is not what makes these acts of intrusion wrongful. They are wrongful because they are demeaning of individuality, and they are such whether or not they cause emotional trauma.

This view of the gravamen of the wrong of intrusion finds support in cases in which courts have expressly rested the right to recover damages for the intrusion on violation of constitutional prohibitions against search and seizure.⁷¹ To be sure, these cases do not say that an unwanted intrusion strikes at one's dignity and offends one's individuality. But the suggestion of this constitutional basis of the right to damages is a step in that direction; at the very least, the cases contradict the view that mental distress is the gist of the action.

Cases in which some form of relief other than damages is sought for an intrusion violating the constitutional prohibition against unreasonable searches and seizures are even closer to the point. The Supreme Court of the United States has declared plainly that the fourth amendment to the federal constitution is designed to protect against intrusions into privacy and that the underlying purpose of such protection is the preservation of individual liberty.⁷² These cases represent, it seems to me, a recognition that unreasonable intrusion is a wrong because it involves a violation of constitutionally protected liberty of the person.

Thus, from the early *Boyd* case⁷³ to the recent case of *Silverman v. United States*,⁷⁴ the Supreme Court has made clear that the "Fourth Amendment gives a man the right to retreat into his own home and there be free from unreasonable governmental intrusion"⁷⁵ and that this right is of "the very essence of constitutional liberty and security."⁷⁶ "The Fourth Amendment," the Court has declared, "forbids

every search that is unreasonable and is construed to safeguard the right of privacy.⁷⁷ Moreover, the Court has proclaimed that "the security of one's privacy against arbitrary intrusion by the police . . . is basic to a free society."⁷⁸

In all of these cases, the intruder was an agent of government and, without doubt, the forms of relief available against a government officer are to be distinguished from those available against intrusions by a private person.⁷⁹ This is not to say, however, that intrusion is a different wrong when perpetrated by an FBI agent and when perpetrated by a next door neighbor; nor is it to say that the gist of the wrong is different in the two cases. The threat to individual liberty is undoubtedly greater when a policeman taps a telephone than when an estranged spouse does, but a similar wrong is perpetrated in both instances. Thus, the conception of privacy generated by the fourth amendment cases may rightly be taken, I would urge, as being applicable to any instance of intrusion even though remedies under the fourth amendment are not available in all such instances.

Brandeis dissent in the *Olmstead* case⁸⁰ is especially instructive in this regard.⁸¹ In that case—decided before the enactment of Section 605 of the Federal Communications Act—the federal government had gained evidence of a violation of the Prohibition Act by tapping a telephone, and the defendant sought to preclude use of the evidence on the theory that it was gained in violation of the fourth amendment. The majority of the Court held that, since the wiretap did not involve a trespass, there was no violation of the fourth amendment and, therefore, the evidence so obtained was legally admissible. **Brandeis** and Holmes dissented.

It is apparent from **Brandeis** dissent that, in the almost forty years which had passed since he had written his article on privacy, he had become as concerned about the evils of unbridled intrusion upon private affairs as he had once been about the evils of unreasonable publicity concerning private affairs. He had also begun to look upon the evils of wiretapping, eavesdropping and the like in the same perspective in which he regarded those attendant upon lurid journalistic exposés of private life.

Modesty seems to have kept him from citing his article, but he nevertheless "lifts" phrases out of it almost verbatim,⁸² and the underlying conceptual scheme is identical. The article was written to thwart threats posed to privacy by "recent inventions and business methods,"⁸³ by "numerous mechanical devices";⁸⁴ the dissent is directed against "far-reaching means of invading privacy"⁸⁵ occasioned by "discovery and invention."⁸⁶ The article seeks to move the common

law in the direction of protecting "man's spiritual nature,"⁸⁷ in the direction of recognizing "thoughts, emotions and sensations"⁸⁸ as objects of legal protection; the dissent attempts to enlarge the sphere of constitutionally protected liberty so as to encompass "man's spiritual nature," and so as "to protect Americans in their beliefs, their thoughts, their emotions and their sensations."⁸⁹

The parallelism between the privacy article and the *Olmstead* dissent is so close as to suggest strongly that **Brandeis** believed, at the time he wrote his dissent, that the fourth amendment was intended to protect the very principle of "inviolate personality" which he had earlier suggested was the principle underlying the common law right to privacy.⁹⁰ More recently, Justice Murphy of the Supreme Court has made this conceptual identification explicit. In his dissent in the *Goldman* case, he said that the "right of personal privacy [is] guaranteed by the Fourth Amendment" and in describing the right he relied upon the Warren-**Brandeis** article, as well as numerous tort cases.⁹¹ The dissents of **Brandeis** and Murphy—and it should be noted that in each of these cases the Court divided over the scope of the protection of the fourth amendment rather than the analysis of the social value it embodies—provide authoritative support for believing that the social interest underlying the "intrusion cases" is that of liberty of the person, the same interest protected by the fourth amendment.

C. The public disclosure cases

The second group of privacy cases to which Dean Prosser addresses himself is that in which there is a public disclosure of facts concerning a person's private life.⁹² Typically, these cases involve a newspaper story, a film, or a magazine article about some aspect of a person's private life. Two of the leading cases are *Melvin v. Reid*⁹³ and *Sidis v. F-R Publishing Corp.*⁹⁴ In the former case, the defendant had made a motion picture using the plaintiff's maiden name and depicting her as a prostitute who had been involved in a sensational murder trial. The scandalous and sensational behavior shown in the film took place many years before it was made and, when the picture was released, the plaintiff was living a conventionally respectable life. The California court upheld a cause of action for the violation of the plaintiff's right to privacy, relying upon the **Warren-Brandeis** article and upon a provision of the California constitution guaranteeing the "inalienable rights" of "enjoying and defending life and liberty; acquiring, possessing, and protecting property; and pursuing and obtaining safety and happiness."⁹⁵

In the *Sidis* case, the New Yorker magazine had published a "profile" of a young man who, years before, had been an infant prodigy, well known to the public, but who, at the time of the article, had retired of his own will and desire into a life of obscurity and seclusion. The article, although true and not unfriendly, was "merciless in its dissection of intimate details of its subject's personal life"⁹⁶ and the court plainly indicated that Sidis' privacy had been invaded.⁹⁷ Recovery was nevertheless denied. Relying on a suggestion in the Warren-Brandeis article that "the interest of the individual in privacy must inevitably conflict with the interest of the public in news," the court concluded that, since Sidis was a "public figure," the "inevitable conflict" had to be resolved in favor of the public interest in news.⁹⁸

After discussing *Melvin v. Reid*, the *Sidis* case and dozens of others like them, Dean Prosser concludes that "this branch of the tort is evidently something quite distinct from intrusion" and that the interest protected in these cases "is that of reputation."⁹⁹ As I have shown above, this analysis is completely at odds with that of Warren and Brandeis.¹⁰⁰ It is also, I believe, at odds with the cases.

What Warren and Brandeis urged, even before the decision of any of the public disclosure cases, about the differences between privacy and defamation makes eminent good sense in the light of the cases themselves,¹⁰¹ and Dean Prosser nowhere attempts to meet it. The public disclosure cases rest on a "radically different principle" than the defamation cases because the former class of cases involves an affront to "inviolate personality" while the latter class of cases involves an impairment of reputation.¹⁰² Moreover, the one class of cases rests on unreasonable publicity, the other on falsity. The right to privacy exists not only "to prevent inaccurate portrayal of private life, but to prevent its being depicted at all."¹⁰³

To be sure, *Melvin v. Reid*¹⁰⁴ and many other of the cases of this type contain express allegations of loss of reputation, of being exposed to public contempt, obloquy, ridicule and scorn as a result of the public disclosure. To my mind, however, such allegations are only incidental to the real wrong complained of, which is the intrusion on privacy, and this wrong, as the *Sidis* case¹⁰⁵ makes apparent, is made out even if the public takes a sympathetic rather than a hostile view of the facts disclosed. What the plaintiffs in these cases complain of is not that the public has been led to adopt a certain attitude or opinion concerning them—whether true or false, hostile or friendly—but rather that some aspect of their life has been held up to public scrutiny at all. In this sense, the gravamen of the complaint here is just like that in the intrusion cases; in effect, the publicity constitutes a form of

intrusion, it is as if 100,000 people were suddenly peering in, as through a window, on one's private life.

When a newspaper publishes a picture of a newborn deformed child,¹⁰⁶ its parents are not disturbed about any possible loss of reputation as a result. They are rather mortified and insulted that the world should be witness to their private tragedy. The hospital and the newspaper have no right to intrude in this manner upon a private life. Similarly, when an author does a sympathetic but intimately detailed sketch of someone, who up to that time had only been a face in the crowd,¹⁰⁷ the cause for complaint is not loss of reputation but that a reputation was established at all. The wrong is in replacing personal anonymity by notoriety, in turning a private life into a public spectacle.

The cases in which undue publicity was given to a debt¹⁰⁸ and in which medical pictures were published¹⁰⁹ are founded on a similar wrong. The complaint is not that people will take a different attitude towards the plaintiff because he owes a debt or has some medical deformity—although they might do so—but rather that publicity concerning these facets of private life represents an imposition upon and an affront to the plaintiff's human dignity.

The essential difference between the cause of action for invasion of privacy by public disclosures and that for defamation is exhibited forcefully by examining how the fact of publication fits into each of the actions. In defamation, publication to even one person is sufficient to make out the wrong.¹¹⁰ In privacy, unless the information was gained by wrongful prying or unless its communication involves a breach of confidence or the violation of an independent duty, some form of mass publication is a requisite of the action. As Dean Prosser himself points out, citing cases in support,

It is an invasion of the right [of privacy] to publish in a newspaper that the plaintiff does not pay his debts, or to post a notice to that effect in a window on the public street or cry it aloud in the highway; but except for one decision of a lower Georgia court which was reversed on other grounds, it has been agreed that it is no invasion to communicate that fact to the plaintiff's employer, or to any other individual, or even to a small group, unless there is some breach of contract, trust or confidential relation which will afford an independent basis for relief.¹¹¹

What at first seem like exceptions to the requirement of mass publication in privacy are easily explained. Where private information is wrongfully gained and subsequently communicated, the wrong is made out independently of the communication. Communication in such a

case, whether to one person or many, is not of the essence of the wrong and only goes to enhance damages. This, then, is not an exception to the rule of mass communication at all. Where, however, a person chooses to give another information of a personal nature on the understanding it will be held private and the confidence is broken, publication is indeed a requisite of recovery and even limited publication is sufficient to support the action. But the wrong here is not the disclosure itself, but rather the disclosure in violation of a relationship of confidence. Disclosure, whether to one person or many, is equally wrongful as a breach of the condition under which the information was initially disclosed.

It is in cases where public disclosure of personal and intimate facts is made without any breach of confidence that the rule of mass disclosure applies in full force. Why should it make a difference in such ~~cases~~^{other} than in the amount of damages recoverable, as it does in defamation actions—whether a statement is published to one or many? Why should it make a difference in determining if an invasion of privacy is made out whether I tell a man's employer he owes me money or whether I shout it from the rooftops? In defamation, a statement is either actionable or not depending upon its subject matter and irrespective of the extent of publication. Why should actionability in privacy sometimes depend upon the extent of publication?

The reason is simply that defamation is founded on loss of reputation while the invasion of privacy is founded on an insult to individuality. A person's reputation may be damaged in the minds of one man or many. Unless there is a breach of a confidential relationship, however, the indignity and outrage involved in disclosure of details of a private life, only arise when there is a massive disclosure, only when there is truly a disclosure to the public.

If a woman who had always lived a life of rectitude were called a prostitute, she could succeed in defamation even if the charge had been made to only one individual. The loss of the respect of that single individual is the wrong complained of. However, absent a breach of confidentiality, if a respectable woman who had once been a prostitute was described as such to a single friend or small group of friends, no cause of action would lie, no matter how radically her friends' opinions changed as a result. The wrong in the public disclosure cases is not in changing the opinions of others, but in having facts about private life made public. The damage is to an individual's self-respect in being made a public spectacle.

The gravamen of a defamation action is engendering a false opinion about a person, whether in the mind of one other person or many

people. The gravamen in the public disclosure cases is degrading a person by laying his life open to public view. In defamation a man is robbed of his reputation; in the public disclosure cases it is his individuality which is lost.

It is admitted that no court has expressed such a view of the series of cases Dean Prosser identifies as public disclosure cases.¹¹² But then no court has adopted Dean Prosser's view of these cases either. The analysis I offer is, however—as I showed above—suggested by the Warren-Brandeis article.¹¹³ Moreover, it finds support in the fact that *Melvin v. Reid*, one of the leading cases of this type, relied upon a constitutional provision guaranteeing life, liberty and happiness.¹¹⁴ Even if this suggestion of a constitutional conceptual basis for privacy is considered "vague,"¹¹⁵ it nevertheless points away from reputation and towards personal dignity and integrity as the gist of the wrong.

Further support for this analysis of the public disclosure cases is found in the fact that it brings these cases into the same framework of theory as the intrusion cases. Many of the intrusion cases rely upon the authority of the public disclosure cases and vice versa.¹¹⁶ If Dean Prosser were correct, such reliance would be mistaken or, at the least, misleading. All else being equal, a theory of the intrusion and public disclosure cases which explains their interdependence and provides a single rationale for them is, I suggest, to be preferred. Physical intrusion upon a private life and publicity concerning intimate affairs are simply two different ways of affronting individuality and human dignity. The difference is only in the means used to threaten the protected interest.

Consider the childbirth situation involved in the *De May* case,¹¹⁷ discussed above. The cause of action there, it will be recalled, was based upon the defendant's having been an unwanted and unauthorized spectator to the plaintiff's birth pangs. To the Michigan court, this was a defilement of what was "sacred."¹¹⁸ But the same sense of outrage, of defilement of what was "sacred," would have ensued if the defendant had been authorized to witness the birth of the plaintiff's child and had subsequently described the scene in detail in the public press. An unwanted report in a newspaper of the delivery room scene, including the cries of anguish and delight, the sometimes abusive, sometimes profane, sometimes loving comments voiced under sedation and the myriad other intimacies of childbirth, would be an insult and an affront of the same kind as an unauthorized physical intrusion upon the scene. The publicity would constitute the same sort of blow to our moral sensibility as the intrusion.

The parallelism which can be constructed in the *De May* case cannot

be constructed in all of the intrusion and publicity cases. Sometimes public disclosure of what is seen or overheard can be offensive and, perhaps, actionable even though the intrusion itself may not be, as, for example, where a reporter "crashes" a private social gathering. Sometimes the details of private life which are publicly reported are not subject to being seen or overheard in a secret or unauthorized fashion at all, as in the case of a debt or a sordid detail of someone's past which is recorded in a public record. However, the fact that public disclosure of information might be actionable even though gaining the information by physical intrusion might not be, or vice versa, is not a ground for believing that the interest protected in each instance is different. The only thing it proves is that publicity concerning personal affairs and physical intrusions upon private life may each be the cause of personal indignity and degradation in ways the other cannot.

The underlying identity of interest in these two branches of the tort was lost sight of, I would suggest, because menacing technological means for intruding upon privacy developed at a later period than threatening forms of public disclosure. Lurid journalism became a fact of American life before the "private eye," the "bug" and the "wiretap." At the time Warren and Brandeis wrote, the common neighborhood snoop was not a sufficient cause for public concern to arouse their interest and the uncommon snoop who uses electronic devices had not yet made his appearance. This possibly explains why their article neglects the three earliest forms of protection against physical intrusions upon privacy, the action in trespass *quare clausum fregit*, "peeping tom" statutes¹¹⁹ and the fourth **amendment**.¹²⁰ However, by the time Brandeis wrote his dissent in the *Olmstead* case,¹²¹ involving a telephone wiretap, the technology of intrusion had developed to the point where he saw that it presented the same threat to individuality as did lurid journalism. As I have already indicated,¹²² Brandeis then drew the necessary consequences for his theory of privacy.

Another aspect of our social history which teaches us something about the gravamen of the public disclosure cases is that Warren and Brandeis did not write their article until 1890, when the American metropolitan press had turned to new forms of sensational reporting and when the social pattern of American life had begun to be set by the mores of the metropolis instead of the small town. A number of writers have recently pointed out that gossip about the private affairs of others is surely as old as human society and that the small town gossip spread the intimacies of one's life with the same energy, skill and enthusiasm as the highest paid reporter of the metropolitan press.¹²³

Why then did it take "recent inventions" and "numerous mechanical devices," the advent of yellow journalism where "gossip... has become a trade,"¹²⁴ to awaken Warren and Brandeis to the need for the right to privacy?

Although the distinction should not be drawn too sharply—the mythology of ruralism is already too deeply embedded—the small town gossip did not begin to touch human pride and dignity in the way metropolitan newspaper gossip mongering does. Resources of isolation, retribution, retraction and correction were very often available against the gossip but are not available to anywhere near the same degree, against the newspaper report. The whispered word over a back fence had a kind of human touch and softness while newsprint is cold and impersonal. Gossip arose and circulated among neighbors, some of whom would know and love or sympathize with the person talked about. Moreover, there was a degree of mutual interdependence among neighbors which generated tolerance and tended to mitigate the harshness of the whispered disclosure.

Because of this context of transmission, small town gossip about private lives was often liable to be discounted, softened and put aside. A newspaper report, however, is spread abroad as part of a commercial enterprise among masses of people unknown to the subject of the report and on this account it assumes an imperious and unyielding influence. Finally, for all of these reasons and others as well, the gossip was never quite believed or was grudgingly and surreptitiously believed, while the newspaper tends to be treated as the very fountain of truth and authenticity, and tends to command open and unquestioning recognition of what it reports.

Thus, only with the emergence of newspapers and other mass means of communication did degradation of personality by the public disclosure of private intimacies become a legally significant reality. The right to sue for defamation has ancient origins because reputation could be put in peril by simple word of mouth or turn of the pen. The right to privacy in the form we know it, however, had to await the advent of the urbanization of our way of life including, as an instance, the institutionalization of mass publicity, because only then was a significant and everyday threat to personal dignity and individuality realized.

D. The use of name or likeness

The third "distinct tort" involving a "distinct interest" which Dean Prosser isolates turns on the commercial exploitation of a person's name or likeness.¹²⁵ This group of cases is designed, he says, to protect

an interest which "is not so much a mental as a proprietary one, in the exclusive use of the plaintiff's name and likeness as an aspect of identity."¹²⁶

In 1902, a flour company circulated Abigail Roberson's photograph, without her consent, as part of an advertising flier and, as a result, she was "greatly humiliated by the scoffs and jeers of persons who recognized her face and picture . . . and her good name had been attacked, causing her great distress and suffering in body and mind."¹²⁷ The New York Court of Appeals, in a 4 to 3 decision, refused recovery because they could find no legal precedent for Warren and Brandeis' right to privacy, on which Abigail relied.¹²⁸ To succeed, the majority indicated, the plaintiff in such a case had to prove either "a breach of trust or that plaintiff had a property right in the subject of litigation which the court could protect,"¹²⁹ and here the plaintiff could show neither.

Three years after the *Roberson* case was decided the same issue came before the Georgia Supreme Court which reached the opposite result. In *Pavesich v. New England Life Ins. Co.*,¹³⁰ the plaintiff's photograph was used, without his consent, in a newspaper advertisement for life insurance, which proclaimed to the world that Pavesich had bought life insurance and was the better man for it. There was no suggestion in the case that the plaintiff sought to vindicate a proprietary interest, that he sought recompense for the commercial value of the use of his name; since he was not well known, the use of his name or picture could hardly command even a fraction of the cost of the lawsuit. Nor did Pavesich claim, as the plaintiff in the *Roberson* case did, that he suffered severe nervous shock as a result of the publication.

The basis of recovery in the case was rather "a trespass upon Pavesich's right of privacy."¹³¹ Relying heavily on the Warren-Brandeis article, the Georgia court recognized the right as derivative of natural law and "guaranteed . . . by the constitutions of the United States and State of Georgia, in those provisions which declare that no person shall be deprived of liberty except by due process of law."¹³² The use of the photograph, declared the court, was an "outrage":

The knowledge that one's features and form are being used for such a purpose and displayed in such places as such advertisements are often liable to be found brings not only the person of an extremely sensitive nature, but even the individual of ordinary sensibility, to a realization that his liberty has been taken away from him, and as long as the advertiser uses him for these purposes, he cannot be otherwise than conscious of the fact that he is, for the time being, under the control of another, and that he is no longer free, and that he is in reality a slave without hope of freedom, held to service by a

merciless master; and if a man of true instincts, or even of ordinary sensibilities, no one can be more conscious of his complete enthrallment than he is.¹³³

The *Pavesich* case has probably been cited more often than any other case in the history of the development of the right to privacy, and it has been cited not only in cases involving use of name or likeness but also in the so-called intrusion cases,¹³⁴ and the public disclosure cases.¹³⁵ To my mind, *Pavesich* and the other use of name or likeness cases are no different in the interest they seek to protect than the intrusion and public disclosure cases. That interest is not, as Dean Prosser suggests,¹³⁶ a "proprietary one," but rather the interest in preserving individual dignity.

The use of a personal photograph or a name for advertising purposes has the same tendency to degrade and humiliate as has publishing details of personal life to the world at large; in the *Pavesich* court's words, the use of a photograph for commercial purposes brings a man "to a realization that his liberty has been taken away from him" and "that he is no longer free."¹³⁷ Thus, a young girl whose photograph was used to promote the sale of dog food complained of "humiliation," "loss of respect and admiration" and Co-incident "mental anguish," and the Illinois court which upheld her cause of action cited the Illinois constitutional guarantee of life, liberty and pursuit of happiness as the basis of recovery.¹³⁸ Similarly, where a lawyer's name was used for the purposes of advertising photocopy equipment,¹³⁹ where a young woman's picture in a bathing suit was used to advertise a slimming product,¹⁴⁰ or where the plaintiff's photograph was used to advertise Doan's pills,¹⁴¹ the wrong complained of was mortification, humiliation and degradation rather than any pecuniary or property loss.

The only difference between these cases and the public disclosure cases is the fact that the sense of personal affront and indignity is provoked by the association of name or likeness with a commercial product rather than by publicity concerning intimacies of personal life. In the public disclosure cases what is demeaning to individuality is being made a public spectacle by disclosure of private intimacies. In these cases what is demeaning and humiliating is the commercialization of an aspect of personality.

One possible cause for confusion concerning the interest which underlies these cases is that the use of name or likeness is held to be actionable in many of the cases precisely because it is a use for commercial or trade purposes. This seems to suggest that the value or interest threatened is a proprietary or commercial one. Such a con-

clusion is mistaken, however, because, in the first place, as I noted above, the name or likeness which is used in most instances has no true commercial value, or it has a value which is only nominal and hardly worth the lawsuit. In fact, it has been held that general rather than special damages are recoverable and this, in itself, is a refutation of the conclusion that the interest concerned is a proprietary one.¹⁴²

In the second place, the conclusion that the plaintiff seeks to vindicate a proprietary right in these cases overlooks the true role of the allegation that the plaintiff's name or picture was used commercially. The reason that the commercial use of a personal photograph is actionable, while—under many circumstances, such as where consent to publication is implied from the fact the photograph was taken in a public place—the use of the same photograph in a news story would not be,¹⁴³ is that it is the very commercialization of a name or photograph which does injury to the sense of personal dignity. As one court has stated, "the right protected is the right to be protected against the commercial exploitation of one's personality."¹⁴⁴

No man wants to be "used" by another against his will, and it is for this reason that commercial use of a personal photograph is obnoxious. Use of a photograph for trade purposes turns a man into a commodity and makes him serve the economic needs and interest of others. In a community at all sensitive to the commercialization of human values, it is degrading to thus make a man part of commerce against his will.¹⁴⁵

Another reason which has possibly led Dean Prosser and others¹⁴⁶ to the conclusion that the interest involved in the use of name or likeness cases is a proprietary one, is that in some few of the cases,¹⁴⁷ the plaintiffs are well known figures whose name or photograph does indeed command a commercial price. In these cases, as Judge Frank has pointed out, the plaintiffs, "far from having their feelings bruised through public exposure of their likenesses, would feel sorely deprived if they no longer received money for authorizing advertisements, popularizing their countenances, displayed in newspapers, magazines, busses, trains and subways."¹⁴⁸

The conclusion to be drawn from such cases, however, is simply that, under special circumstances, as where the plaintiff is a public figure, the use of his likeness or name for commercial purposes involves the appropriation of a thing of value. But it is important to note that, in this respect, such cases are distinguishable from cases like *Pavesich*¹⁴⁹ and *Eick*,¹⁵⁰ for instance, where the plaintiff had no public renown. In other words, the use of a name or likeness only involves an appropriation of a thing of value in a limited class of cases

where: the plaintiff is known to the public and where his name or likeness commands a price.

Some have said that in such cases a "right of publicity" rather than a right of privacy is involved.¹⁵¹ It is a mistake, however, to conclude from these "right of publicity" cases that all the cases involving commercial use of name or likeness are founded on a proprietary interest.¹⁵² Moreover, the very characterization of these cases as involving a "right to publicity" disguises the important fact that name and likeness can only begin to command a commercial price in a society which recognizes that there is a right to privacy, a right to control the conditions under which name and likeness may be used. Property becomes a commodity subject to be bought and sold only where the community will enforce an individual's right to maintain use and possession of it as against the world. Similarly, unless an individual has a right to prevent another from using his name or likeness commercially, even where the use of that name or likeness has no commercial value, no name or likeness could ever command a price.

Thus, there is really no "right to publicity"; there is only a right, under some circumstances, to command a commercial price for abandoning privacy. Every man has a right to prevent the commercial exploitation of his personality, not because of its commercial worth, but because it would be demeaning to human dignity to fail to enforce such a right. A price can be had in the market place by some men for abandoning it, however. If a commercial use is made of an aspect of the personality of such a man without his consent, he has indeed suffered a pecuniary loss, but the loss concerned is the price he could command for abandoning his right to privacy. The so-called "right to publicity" is merely a name for the price for which some men can sell their right to maintain their privacy.

Undoubtedly, there will be cases in which the publication of a name or likeness without consent is a boon and not a burden. Rather than suffering humiliation and degradation as a result, the beautiful but unknown girl pictured on the cover of a nationally circulated phonograph record might be delighted at having been transfigured into a modern Cinderella. Suddenly, she is a national figure, glowing in the limelight, and her picture and name have become sought after commodities as a result. Has privacy been violated when there is no personal sense of indignity and the commercial values of name or likeness have been enhanced rather than diminished?

I believe that in such a case there is an invasion of privacy, although it is obviously not one which will be sued on and not one which is liable to evoke community sympathy or command anything but a

nominaljury award. The case is very much like one in which a physician successfully treats a patient but is held liable for the technical tort of battery because the treatment extended beyond the consent.¹⁵³ However beneficent the motive, or successful the result, the "touching" is considered wrongful. As I view the matter, using a person's name or likeness for a commercial purpose without consent is a wrongful exercise of dominion over another even though there is no subjective sense of having been wronged, even, in fact, if the wrong was subjectively appreciated, and even though a commercial profit might accrue as a result. This is so because the wrong involved is the objective diminution of personal freedom rather than the infliction of personal suffering or the misappropriation of property.

I agree with Dean Prosser that, in one sense, it is "quite pointless to dispute over whether such a right is to be classified as 'property'",¹⁵⁴ as Warren and Brandeis long ago pointed out, there is a sense in which there inheres "in all . . . rights recognized by the law . . . the quality of being owned or possessed—and (as that is the distinguishing attribute of property) there may be some propriety in speaking of those rights as property."¹⁵⁵

But in one sense it is very important, as Warren and Brandeis saw, to decide whether the right to damages for the commercial use of name or likeness is called a property right. The importance resides in finding the common ground between the use of name and likeness cases, the public disclosure cases and the intrusion cases. In Dean Prosser's view the interest vindicated in each of these classes of cases is a different one. In my view the interest protected in each is the same, it is human dignity and individuality or, in Warren and Brandeis' words, "inviolate personality."

E. The "false light" cases

The fourth and final distinct group of cases which Dean Prosser identifies within the overall rubric of privacy are cases which he describes as involving "publicity falsely attributing to the plaintiff some opinion or utterance,"¹⁵⁶ cases in which "the plaintiff's picture [is used] to illustrate a book or an article with which he has no reasonable connection"¹⁵⁷ or in which "the plaintiff's name, photograph and fingerprints [are included] in a public 'rogues' gallery' of convicted criminals, when he has not in fact been convicted of any crime."¹⁵⁸ He says these cases all involve reputation and "obviously differ from those of intrusion, or disclosure of private facts [or appropriation]."¹⁵⁹

I agree with Dean Prosser that all of these cases involve reputation,

but I am persuaded, though he is not, that they also involve the assault on individual personality and dignity which is characteristic of all the other privacy cases. The slur on reputation is an aspect of the violation of individual integrity.

Two California cases in which Mr. and Mrs. Gill sued for damages illustrate the point. They were photographed embracing in their place of business and the photograph was used in two different articles in the public press on the subject of love. In one of the articles, the photograph was used to illustrate the "wrong kind of love" consisting "wholly of sexual attraction and nothing else." In the other article, the photograph was used without any particular portion of the text referring to it. The plaintiffs succeeded against the publisher who characterized their love as being of the "wrong kind,"¹⁶⁰ but their complaint was dismissed as against the other publisher.¹⁶¹

The use of a photograph taken in a public place and published without comment in a news article could not be considered offensive to personal dignity because consent to such a publication, to the abandonment of privacy, is implied from the fact the Gills embraced in public. Use of the same photograph accompanied by false and derogatory comment is another matter, however. Although the comment may not be defamatory and, therefore, not actionable as such, when combined with the public exploitation of the photograph, it turns the otherwise inoffensive publication into one which is an undue and unreasonable insult to personality. It is the combination of false and stigmatic comment on character with public exhibition of the photograph which constitutes the actionable wrong.

Publishing a photograph in a "false light" serves the same function in constituting the wrong as does a use of the photograph for advertising purposes. The picture of Mr. and Mrs. Gill embracing could no more be used to cast aspersions on the character of their love than it could be used to advertise the aphrodisiac effects of a perfume. In both instances, such publicity "violates the ordinary decencies"¹⁶² and impinges on their right to maintain their identity as individuals. (Significantly, the California District Court of Appeals which upheld the Gills' action cited a section of the California constitution guaranteeing the right to pursue and gain happiness¹⁶³ which is almost identical to the section of the Georgia constitution cited in the *Pavesich* case,¹⁶⁴ involving an unauthorized use of a photograph for advertising purposes.)

The use of a name in a "false light" is actionable for the same reasons as the use of a name for a commercial purpose. The "false light" in which the name is used makes the use wrongful for the same reason

that the use of the name for advertising purposes does. And, in fact, many of the cases which Dean Prosser cites as actionable for "falsely attributing to the plaintiff some opinion or utterance"¹⁶⁵—including the leading *Pavesich* case¹⁶⁶—are cases in which a name has been used for advertising purposes.

I suspect that the reason which leads Dean Prosser to distinguish the "false light" cases from the use of name and likeness cases is that, as I indicated above,¹⁶⁷ he mistakenly regards the latter group of cases as turning on a proprietary interest in name or likeness. If you believe the use for advertising purposes of a photograph of two ordinary people embracing is wrongful because it violates their pecuniary interest in their name or likeness, you will regard the use of the same photograph in a "false light"—illustrating a depraved kind of love-making, for instance—as involving a fundamentally different kind of wrong. However, once it is recognized that the use of a name for advertising purposes is wrongful because it is an affront to personal dignity,¹⁶⁸ the underlying similarity between the advertising and "false light" cases becomes apparent. The "false light" and the advertising use are merely two different means of publishing a person's name or likeness so as to offend his dignity as an individual.

There is a recent tendency in the law of defamation which has extended the interest protected by that cause of action beyond the traditional reaches of character to include aspects of personal humiliation and degradation.¹⁶⁹ The cases pointing in this direction are those, for instance, in which recovery in libel has been allowed to a man whose published photograph represented him as grossly deformed¹⁷⁰ and in which recovery was allowed for publishing a photograph of an English sports amateur so as to suggest that he was commercially advertising chocolate.¹⁷¹ These cases, it has been said, "have made it possible to reach certain indecent violations of privacy by means of the law of libel, on the theory that any writing is a libel that discredits the plaintiff in the minds of any considerable and respectable class in the community though no wrongdoing or bad character is imputed to him."¹⁷²

This tendency in the law of defamation is consistent with, is, in fact, the counterpart of, the growth of the "false light" category of recovery in the law of privacy. It strongly suggests that the law of privacy may provide a valuable avenue or development for the law of defamation.¹⁷³ In this sense, however, it is the law of privacy which helps explain the defamation cases, rather than vice versa, as Dean Prosser suggests.

IV. Privacy in non-tort contexts

Besides introducing four principles to explain the tort cases involving privacy 'where one will suffice, Dean Prosser's analysis also has the unfortunate consequence that it makes impossible the reconciliation of privacy in tort and non-tort contexts. If privacy in tort is regarded as an amalgam of the infliction of emotional distress, defamation and misappropriation, it is impossible to find any common link between the tort cases and various forms of protection of privacy which are found in constitutions, statutes and common law rules which do not involve tort claims.

Actually, however, there is a common thread of principle and an identical interest or social value which runs through the tort cases as well as the other forms of legal protection of privacy. Thus, for instance, as I have already shown,¹⁷⁴ the fourth amendment to the federal constitution erects a barrier against unreasonable governmental entries into a man's home or searches of his person, and the Supreme Court has indicated on many occasions that this protection is of the very essence of constitutional liberty and security.¹⁷⁵ If the gravamen of intrusion as a tort is said to be the intentional infliction of emotional distress, the conceptual link between the tort and the fourth amendment is lost. But if the intrusion cases in tort are regarded as involving a blow to human dignity or an injury to personality, their relation to the constitutional protection of the fourth amendment becomes apparent.

The difference between the *De May* case,¹⁷⁶ involving an unauthorized witness to childbirth, and the *Silverman* case,¹⁷⁷ involving the use of a "spike" microphone in a criminal investigation to overhear a conversation in a home, is that the former involved an intrusion by a private person and a tort remedy was sought, while the latter involved an intrusion by a government agent and the remedy sought was the suppression of the use of the fruits of the intrusion. But the underlying wrong in both instances was the same; the act complained of was an affront to the individual's independence and freedom. A democratic state which values individual liberty can no more tolerate an intrusion on privacy by a private person than by an officer of government and the protections afforded in tort law, like those afforded under the Constitution, are designed to protect this same value.

A similar analysis may also be made of the public disclosure cases, the use of name or likeness cases and the "false light" cases. In these

cases the individual's dignity has been subject to challenge just as it was in the *Silberman* case, the *De May* case and the other intrusion cases. Respect for individual liberty not only commands protection against intruders into a person's home but also against making him a public spectacle by undue publicity concerning his private affairs or degrading him by commercializing his name or likeness or using it in a "false light." Each of these wrongs constitutes an intrusion on personality, an attack on human dignity.

It is true, of course, that the fourth amendment only protects against invasions of privacy perpetrated by state or federal officers.¹⁷⁸ This does not mean, however, that the wrong against which the amendment was erected is different from that which is involved where one private citizen intrudes upon another's home or subjects his person to an unwarranted search. Moreover, each state has a search and seizure provision comparable to that of the fourth amendment¹⁷⁹ and, in some states at least, it has been held that the provision applies to private persons.¹⁸⁰

Thus, the protection which the fourth amendment secures against the enforcement of the criminal law by means of unreasonable searches and seizures involves the same underlying interest as that secured by the right of privacy in tort law. Although there are undoubtedly other considerations of policy involved in the fourth amendment cases,¹⁸¹ they, like the tort cases, are intended to preserve individual dignity.

This same value is also enforced in numerous statutes which make intrusions on privacy a crime. The oldest of such are the so-called "peeping tom" statutes, which make it a misdemeanor to peer into the window of another's home.¹⁸² The introduction of new means of "peeping," of electronic means of eavesdropping, has brought forth modern versions of the older "peeping tom" statutes. The Federal Communications Act makes it a crime to listen in to a telephone conversation without consent by tapping the telephone and subsequently disclosing what is heard.¹⁸³ And in New York, Illinois and Nevada it is a crime to eavesdrop "by means of instrument" on any conversation, telephonic or otherwise, or even to possess eavesdropping equipment.¹⁸⁴

These statutes are obviously aimed at the same wrong against which the common law intrusion cases discussed above are directed.¹⁸⁵ Some of them provide for a civil remedy as well as a criminal penalty and thereby expressly enlarge the tort right to privacy.¹⁸⁶ Some courts have engrafted a civil remedy on the criminal prohibition, using the criminal statute—as is frequently done in the law of tort¹⁸⁷—to define the wrong for which recompense in damages may be sought.¹⁸⁸

Thus, for instance, in *Reitmaster v. Reitmaster*,¹⁸⁹ the defendants had violated the provisions against wiretapping in Section 605 of the Federal Communications Act and the plaintiff sued for damages. Although a jury verdict in favor of the defendant based on a finding of consent was affirmed, Judge Learned Hand, writing for the Second Circuit Court of Appeals, plainly indicated that a civil suit for damages would lie for a breach of Section 605. He said:

Although the Act does not expressly create any civil liability, we can see no reason why the situation is not within the doctrine which, in the absence of contrary implications, construes a criminal statute, enacted for the benefit of a specified class, as creating a civil right in members of the class, although the only express sanctions are criminal.¹⁹⁰

Such judicial creation of a civil remedy on the basis of the criminal wrong of wiretapping or eavesdropping, read together with the eavesdropping statutes which expressly provide coordinate civil and criminal remedies,¹⁹¹ proves the identity of interest behind the civil and criminal remedies. It also provides an added reason for disputing Dean Prosser's contention¹⁹² that the wrong in such intrusion cases is the intentional infliction of mental distress; if it were, the civil remedy would only be available on a showing of such distress, but, in fact, there is no such requirement. Finally, it should be noted that the theory expressed by Judge Hand in *Reitmaster* would provide an easy avenue for extending the civil right of privacy in New York, where it is a creature of a statute which limits recovery of damages to the use of name or likeness for purposes of trade or advertising.¹⁹³

Another important class of statutes which are intended to protect against degradation of individuality are those which prohibit the disclosure of confidential information of various sorts. Thus, for instance, we are all required by law to divulge a great deal of information—of a personal as well as of a business nature—to the United States Government for the purpose of the census.¹⁹⁴ But all such information is made confidential by statute and unauthorized disclosure of it is a crime.¹⁹⁵ Although it is not as comprehensive, a similar prohibition against disclosure of data concerning personal lives and business affairs given for purposes of tax collection is to be found in the Internal Revenue Code.¹⁹⁶ And, in Title 18 of the United States Code, there is a broad prohibition, backed by criminal penalty, against disclosure by a federal officer of a wide range of confidential information concerning the operation of businesses.¹⁹⁷

Similar statutes are to be found in state law. New York, for example, has a provision in its Public Officer's Law, which is not enforced by

a criminal penalty, forbidding any public officer from disclosing confidential information acquired in the course of his official duties.¹⁹⁸ In the Penal Law, there are provisions making it a crime for an employee of a telegraph or telephone company to divulge information gained in the course of his employment.¹⁹⁹ In another section of the Penal Law, disclosure by an election officer or poll watcher of the name of the candidate for whom a person has voted is made a misdemeanor.²⁰⁰ In the Social Welfare Law, publication of the names of people receiving or applying for public assistance is made a crime, and all information obtained by and communications to a public welfare official, as well as all records of abandoned or delinquent children, are made confidential.²⁰¹

The same pattern of protection is found in still other New York statutes. Thus, the Correction Law contains provisions intended to preserve the confidential character of criminal identification records and statistics.²⁰² The General Business Law forbids an employee of a licensed private investigator to divulge information gathered by his employer.²⁰³ The Civil Rights Law forbids the publication of testimony taken in private by certain state investigative agencies.²⁰⁴ And, finally, the Education Law forbids soliciting, receiving or giving information concerning persons applying for vocational rehabilitation training.²⁰⁵

This brief survey of federal and New York State statutes regulating disclosure of confidential information is not, of course, intended to be exhaustive. My purpose is rather to demonstrate by these statutes—and it should be noted that there are undoubtedly untold administrative regulations on the federal and state level which have a similar purport—that the same impetus which moved the common law courts to erect a civil cause of action founded on public disclosure of aspects of private life²⁰⁶ also provoked action by the national and state legislatures intending to serve the same purpose.

Following Warren and Brandeis' lead, the common law courts responded to the threat posed to privacy by lurid journalism and demeaning advertising. Legislatures have responded to threats to personal dignity which were not yet manifest when Warren and Brandeis wrote. It was only after the turn of the century that the telephone and telegraph became instruments of everyday life, used to confide personal intimacies and business secrets. Unless some security could be found against people illicitly breaking in upon these private communications and divulging what was learned, an important area of private life would be subject to degrading public scrutiny, and public confidence in these instruments of communication would be destroyed. Section 605 of the Federal Communications Act²⁰⁷ and var-

ious state statutes²⁰⁸ were intended to prevent this consequence. Whether they were successful or not is, of course, another question.

Another avenue for impairing the privacy of our lives—again one which only became a cause for public concern after Warren and Brandeis wrote—was the increasing accumulation of information about each of us which finds its way into government records and files. Of course, the very fact that a government agency requires such information under the compulsion of law,²⁰⁹ whether for the purposes of providing social welfare benefits, taking the census, or collecting taxes, is itself an intrusion upon our persons. Most of us have agreed, however, that the social benefit to be gained in these instances require the information to be given and that the ends to be achieved are worth the price of diminished privacy.

But this tacit agreement is founded upon an assumption that information given for one purpose will not be used for another.²¹⁰ We are prepared to tell the tax collector and the census taker what they need to know, but we are not prepared to have them make a public disclosure of what they have learned. The intrusion is tolerable only if public disclosure of the fruits of the intrusion is forbidden. This explains why many of the statutes which require us to tell something about ourselves to a government agency contain an express provision against disclosure of such information.²¹¹ It also explains why there are general provisions prohibiting disclosure of information of a personal nature gained in an official capacity.²¹² Again, I note that my purpose here is not to comment upon the effectiveness of these anti-disclosure statutes; it is only to describe their broad aims.

The parallelism between the intrusion and the disclosure statutes, on the one hand, and the intrusion and disclosure tort cases, on the other, illuminates, I believe, the common conceptual character of privacy which runs through all of them. Intrusion and public disclosure are merely alternative forms of injury to individual freedom and dignity. The common law courts provide civil relief against turning a man's private life into a public spectacle as well as against impairing his private intimacies by intruding upon them.²¹³ Similarly, legislatures have been impelled to prevent both eavesdropping and *divulgence*²¹⁴ or, where the intrusion is socially sanctioned, as in the census and tax fields, disclosure for other than sanctioned purposes. The disclosure provisions of the statutes, like the tort disclosure cases, preserve dignity by restricting publicity, by assuring a man that his life is not the open and indiscriminate object of all eyes. And, as the comparable tort cases do in relation to the tort intrusion cases, the statutory disclosure provisions complement the statutory intrusion provisions by

making a man secure in his person, not only against prying eyes and ears, but against the despair of being the subject of public scrutiny and knowledge.

V. Conclusion: the invasion of privacy as an affront to human dignity

Dean Prosser has described the privacy cases in tort as involving "not one tort, but a complex of four,"²¹⁵ as "four disparate torts under . . . [a] common name."²¹⁶ And he believes that the reason the state of the law of privacy is "still that of a haystack in a hurricane," as Chief Judge Biggs said in *Ettore v. Philco Television Broadcasting Co.*,²¹⁷ is that we have failed to "separate and distinguish" these four torts.²¹⁸

I believe to the contrary that the tort cases involving privacy are of [one piece and involve a single tort. Furthermore, I believe that a common thread of principle runs through the tort cases, the criminal cases involving the rule of exclusion under the fourth amendment, criminal statutes prohibiting peeping toms, wiretapping, eavesdropping, the possession of wiretapping and eavesdropping equipment, and criminal statutes or administrative regulations prohibiting the disclosure of confidential information obtained by government agencies.

The words we use to identify and describe basic human values are necessarily vague and ill-defined. Compounded of profound human hopes and longings on the one side and elusive aspects of human psychology and experience on the other, our social goals are more fit to be pronounced by prophets and poets than by professors. We are fortunate, then, that some of our judges enjoy a touch of the prophet's vision and the poet's tongue.

Before he ascended to the bench, Justice Brandeis had written that the principle which underlies the right to privacy was "that of an inviolate personality."²¹⁹ Some forty years later, in the *Olmstead* case,²²⁰ alarmed by the appearance of new instruments of intrusion upon "inviolate personality," he defined the threatened interest more fully.

The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feeling and of his intellect. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.²²¹

Other Justices of our Supreme Court have since repeated, elucidated and expanded upon this attempt to define privacy as an aspect of the pursuit of happiness.²²²

More obscure judges, writing in the more mundane context of tort law, have witnessed this same connection. In two of the leading cases in the field, *Melvin v. Reid*²²³ and *Pavesich v. New England Life Ins. Co.*²²⁴—one a so-called public disclosure case; the other a so-called appropriation or "false light" case—the right to recovery was founded upon the state constitutional provision insuring the pursuit of happiness.²²⁵ Judge Cobb, writing in *Pavesich*, declared:

An individual has a right to enjoy life in any way that may be most agreeable and pleasant to him, according to his temperament and nature, provided that in such enjoyment he does not invade the rights of his neighbor or violate public law or policy. The right of personal security is not fully accorded by allowing an individual to go through his life in possession of all his members and his body unmarred; nor is his right to personal liberty fully accorded by merely allowing him to remain out of jail or free from other physical restraints. . . .

Liberty includes the right to live as one will, so long as that will does not interfere with the rights of another or of the public. One may desire to live a life of seclusion; another may desire to live a life of publicity; still another may wish to live a life of privacy as to certain matters and of publicity as to others. . . . Each is entitled to a liberty of choice as to his manner of life, and neither an individual nor the public has a right to arbitrarily take away from him his liberty.²²⁶

Some may find these judicial visions of the social goal embodied in the right to privacy vague and unconvincing. I find them most illuminating. Unfortunately, the law's vocabulary of mind is exceedingly limited. Our case law too often speaks of distress, anguish, humiliation, despair, anxiety, mental illness, indignity, mental suffering, and psychosis without sufficient discrimination of the differences between them. Justice Brandeis and Judge Cobb help us see, however, that the interest served in the privacy cases is in some sense a spiritual interest rather than an interest in property or reputation. Moreover, they also help us understand that the spiritual characteristic which is at issue is not a form of trauma, mental illness or distress, but rather individuality or freedom.

An intrusion on our privacy threatens our liberty as individuals to do as we will, just as an assault, a battery or imprisonment of our person does. And just as we may regard these latter torts as offenses "to the reasonable sense of personal dignity,"²²⁷ as offensive to our

concept of individualism and the liberty it entails, so too should we regard privacy as a dignitary tort.²²⁸ Unlike many other torts, the harm caused is not one which may be repaired and the loss suffered is not one which may be made good by an award of damages. The injury is to our individuality, to our dignity as individuals, and the legal remedy represents a social vindication of the human spirit thus threatened rather than a recompense for the loss suffered.

What distinguishes the invasion of privacy as a tort from the other torts which involve insults to human dignity and individuality is merely the means used to perpetrate the wrong. The woman who is indecently pelted²²⁹ suffers the same indignity as the woman whose birth pangs are overseen.²³⁰ The woman whose photograph is exhibited for advertising purposes²³¹ is degraded and demeaned as surely as the woman who is kept aboard a pleasure yacht against her will.²³² In all of these cases there is an interference with individuality, an interference with the right of the individual to do what he will. The difference is in the character of the interference. Whereas the affront to dignity in the one category of cases is affected by physical interference with the person, the affront in the other category of cases is affected, among other means, by physically intruding on personal intimacy and by using techniques of publicity to make a public spectacle of an otherwise private life.

The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual.

The conception of man embodied in our tradition and incorporated in our Constitution stands at odds to such human fungibility. And our law of privacy attempts to preserve individuality by placing sanctions upon outrageous or unreasonable violations of the conditions of its sustenance. This, then, is the social value served by the law of privacy, and it is served not only in the law of tort, but in numerous other areas of the law as well.

To be sure, this identification of the interest served by the law of privacy does not of itself "solve" any privacy problems; it does not furnish a ready-made solution to any particular case of a claimed invasion of privacy. In the first place, not every threat to privacy is

of sufficient moment to warrant the imposition of civil liability or to evoke any other form of legal redress. We all are, and of necessity must be, subject to some minimum scrutiny of our neighbors as a very condition of life in a civilized community. Thus, even having identified the interest invaded, we are left with the problem whether, in the particular instance, the intrusion was of such outrageous and unreasonable character as to be made actionable.

Secondly, even where a clear violation of privacy is made out, one must still face the question whether it is not privileged or excused by some countervailing public policy or social interest. The most obvious such conflicting value is the public interest in news and information which, of necessity, must sometimes run counter to the individual's interest in privacy.²³³ Again, identification of the nature of the privacy interest does not resolve the conflict of values, except insofar as it makes clear at least one of the elements which is to be weighed in the balance.

One may well ask, then, what difference it makes whether privacy is regarded as involving a single interest, a single tort, or four? What difference whether the tort of invasion of privacy is taken to protect the dignity of man and whether this same interest is protected in non-tort privacy contexts?

The study and understanding of law, like any other study, proceeds by way of generalization and simplification. To the degree that relief in the law courts under two different sets of circumstances can be explained by a common rule or principle, to that degree the law has achieved greater unity and has become a more satisfying and useful tool of understanding. Conceptual unity is not only fulfilling in itself, however; it is also an instrument of legal development.

Dean Prosser complains of "the extent to which defenses, limitations and safeguards established for the protection of the defendant in other tort fields have been jettisoned, disregarded, or ignored" in the privacy cases.²³⁴ Because he regards intrusion as a form of the infliction of mental distress, it comes as a surprise and cause for concern that the courts, in the intrusion cases, have not insisted upon "genuine and serious mental harm," the normal requirement in the mental distress cases.²³⁵ Because he believes the public disclosure cases and the "false light" cases involve injury to reputation, he is alarmed that the courts in these cases have jettisoned numerous safeguards—the defense of truth and the requirement, in certain cases, of special damages, for instance—which were erected in the law of defamation to preserve a proper balance between the interest in reputation and the interest in a free press.²³⁶ And because he conceives of the use of name and likeness cases as involving a proprietary interest in name

or likeness comparable to a common law trade name or trademark, he is puzzled that there has been "no hint" in these cases "of any of the limitations which have been considered necessary and desirable in the ordinary law of trade-marks and trade names."²³⁷

The reason for Dean Prosser's concern and puzzlement in each instance is based on his prior identification of the interest the tort remedy serves. If the intrusion cases serve the purpose of protecting emotional tranquility, certain legal consequences concerning necessary allegations and defenses appropriate to the protection of that interest seem to follow. The same is true for the other categories of cases as well. If he is mistaken in his identification of the interest involved in the privacy cases, however, the development of the tort will take—actually, as I have shown above, it has already taken—an entirely different turn, and will have entirely different dimensions.

The interest served by the remedy determines the nature of the cause of action and the available defenses because it enters into the complex process of weighing and balancing of conflicting social values which courts undertake in affording remedies. Therefore, my suggestion that all of the tort privacy cases involve the same interest in preserving human dignity and individuality has important consequences for the development of the tort. If this, rather than emotional tranquility, reputation or the monetary value of a name or likeness is involved, courts will be faced by the need to compromise and adjust an entirely different set of values, values more similar to those involved in battery, assault and false imprisonment cases than in mental distress, defamation and misappropriation cases.

The identification of the social value which underlies the privacy cases will also help to determine the character of the development of new legal remedies for threats posed by some of the aspects of modern technology. Criminal statutes which are intended to curb the contemporary sophisticated electronic forms of eavesdropping and evidentiary rules which forbid the disclosure of the fruits of such eavesdropping can only be assimilated to the common law forms of protection against intrusion upon privacy if the social interest served by the common law is conceived of as the preservation of individual dignity. These statutes are obviously not designed to protect against forms of mental illness or distress and to so identify the interest involved in the common law intrusion cases is to rob the argument for eavesdropping statutes of a valuable source of traditional common law analysis.

A similar argument may be made concerning other contemporary tendencies in the direction of stripping the individual naked of his human dignity by exposing his personal life to public scrutiny. The

personnel practices of government and large-scale corporate enterprise increasingly involve novel forms of investigation of personal lives. Extensive personal questionnaires, psychological testing and, in some instances, the polygraph have been used to delve deeper and deeper into layers of personality heretofore inaccessible to all but a lover, an intimate friend or a physician. And the information so gathered is very often stored, correlated and retrieved by electronic machine techniques. The combined force of the new techniques for uncovering personal intimacies and the new techniques of electronic use of this personal data threatens to uncover inmost thoughts and feelings never even "whispered in the closet" and to make them all too easily available "to be proclaimed from the housetops."²³⁸

The character of the problems posed by psychological testing, the polygraph and electronic storage of personal data can better be grasped if seen in the perspective of the common law intrusion and disclosure cases. The interest threatened by these new instruments is the same as that which underlies the tort cases. The feeling of being naked before the world can be produced by having to respond to a questionnaire or psychological test as well as by having your bedroom open to prying eyes and ears. And the fear that a private life may be turned into a public spectacle is greatly enhanced when the lurid facts have been reduced to key punches or blips on a magnetic tape accessible, perhaps, to any clerk who can throw the appropriate switch.

This is not to say, of course, that the same adjustments of conflicting values which have been made in the tort privacy cases can be assumed to apply without modification to resolve the questions of public policy raised by the use of sophisticated electronic eavesdropping equipment, psychological techniques of probing the individual psyche or the electronic data processing equipment. Nor is to say that the expansion of the tort remedy will provide a satisfactory legal or social response to these new problems. It is rather only to say that, in both instances, community concern for the preservation of the individual's dignity is at issue and that the legal tradition associated with resolving the one set of problems is available for us in resolving the other.

NOTES

- 1 Warren & Brandeis, *The Right of Privacy*, 4 Harv. L. Rev. 193 (1890) [hereinafter cited as Warren & Brandeis].
- 2 See, e.g., Annot., 138 A.L.R. 22 (1942); Annot., 168 A.L.R. 446 (1947); Annot., 14 A.L.R.2d 750 (1950).



Governments Haven't Shown Location Surveillance Would Help Contain COVID-19

Governments around the world are demanding new dragnet location surveillance powers to contain the COVID-19 outbreak. But before the public allows their governments to implement such systems, governments must explain to the public how these systems would be effective in stopping the spread of COVID-19. There's no questioning the need for far-reaching public health measures to meet this urgent challenge, but those measures must be scientifically rigorous, and based on the expertise of public health professionals.

Governments have not yet met that standard, nor even shown that extraordinary location surveillance powers would make a significant contribution to containing COVID-19. Unless they can, there's no justification for their intrusions on privacy and free speech, or the disparate impact these intrusions would have on vulnerable groups. Indeed, governments have not even been [transparent](#) about their plans and rationales.

The Costs of Location Surveillance

EFF has [long opposed](#) location surveillance programs that can turn our lives into [open books](#) for scrutiny by police, surveillance-based advertisers, identity thieves, and stalkers. Many sensitive inferences can be drawn from a visit to a health center, a criminal defense lawyer, an immigration clinic, or a protest planning meeting.

Moreover, fear of surveillance [chills and deters](#) free speech and association. And [all too often](#), surveillance disproportionately burdens people of color. What's more, whatever personal data is collected by government can be [misused](#) by its

employees, stolen by criminals and foreign governments, and unpredictably redirected by agency leaders to harmful new uses.

Emerging Dragnet Location Surveillance

China reportedly responded to the COVID-19 crisis by building new infrastructures to track the movements of massive numbers of identifiable people. Israel tapped into a vast trove of cellphone location data to identify people who came into close contact with known virus carriers. That nation has sent quarantine orders based on this surveillance. About a dozen countries are reportedly testing a spy tool built by NSO Group that uses huge volumes of cellphone location data to match the location of infected people to other people in their vicinity (NSO's plan is to not share a match with the government absent such a person's consent).

In the United States, the federal government is reportedly seeking, from mobile app companies like Facebook and Google, large volumes of location data that is de-identified (that is, after removal of information that identifies particular people) and aggregated (that is, after combining data about multiple people). According to industry executives, such data might be used to predict the next virus hotspot. Facebook has previously made data like this available to track population movements during natural disasters.

But re-identification of de-identified data is a constant infosec threat. De-identification of location data is especially hard, since location data points serve as identification of their own. Also, re-identification can be achieved by correlating de-identified data with other publicly available data like voter rolls, and with the oceans of information about identifiable people that are sold by data brokers. While de-identification might in some cases reduce privacy risks, this depends on many factors that have not yet been publicly addressed, such as careful selection of what data to aggregate, and the minimum thresholds for aggregation. In the words of Prof. Matt Blaze, a specialist in computer science and privacy:

One of the things we have learned over time is that something that seems anonymous, more often than not, is not anonymous, even if it's designed with the best intentions.

Disturbingly, most of the public information about government's emerging location surveillance programs comes from anonymous sources, and not official explanations. Transparency is a cornerstone of democratic governance, especially

now, in the midst of a public health crisis. If the government is considering such new surveillance programs, it must publicly explain exactly what it is planning, why this would help, and what rules would apply. History shows that when government builds new surveillance programs in secret, these programs quickly lead to unjustified privacy abuses. That's one reason EFF has long demanded transparent democratic control over whether government agencies may deploy new surveillance technology.

Governments Must Show Their Work

Because new government dragnet location surveillance powers are such a menace to our digital rights, governments should not be granted these powers unless they can show the public how these powers would actually help, in a significant manner, to contain COVID-19. Even if governments could show such efficacy, we would still need to balance the benefit of the government's use of these powers against the substantial cost to our privacy, speech, and equality of opportunity. And even if this balancing justified government's use of these powers, we would still need safeguards, limits, auditing, and accountability measures. In short, new surveillance powers must always be necessary and proportionate.

But today, we can't balance those interests or enumerate necessary safeguards, because governments have not shown how the proposed new dragnet location surveillance powers could help contain COVID-19. The following are some of the points we have not seen the government publicly address.

- 1. Are the location records sought sufficiently granular to show whether two people were within transmittal distance of each other?** In many cases, we question whether such data will actually be useful to healthcare professionals.

This may seem paradoxical. After all, location data is sufficiently precise for law enforcement to place suspects at the scene of a crime, and for juries to convict largely on the basis of that evidence. But when it comes to tracking the spread of a disease that requires close personal contact, data generated by current technology generally can't reliably tell us whether two people were closer than the CDC-recommended radius of six feet for social distancing.

For example, cell site location information (CSLI)—the records generated by mobile carriers based on which cell towers a phone connects to and when—is often only able to place a phone within a zone of half a mile to two miles in urban areas. The area is even wider in areas with less dense tower placement. GPS sensors built directly into phones can do much better, but even GPS is only

accurate to a [16-foot radius](#). These and other technologies like Bluetooth can be combined for better accuracy, but there's no guarantee that a given phone can be located with six-foot precision at a given time.

2. Do the cellphone location records identify a sufficiently large and representative portion of the overall population? Even today, not everyone has a cellphone, and some people do not regularly carry their phones or connect them to a cellular network. The population that carries a networked phone at all times is not representative of the overall population; for example, people without phones skew towards [lower-income](#) people and [older](#) people.

3. Has the virus already spread [so broadly](#) that contact tracing is no longer a significant way to reduce transmission? If community transmission is commonplace, contact tracing may become [impractical](#) or divert resources from more effective containment methods.

There might be scenarios other than precise, person-to-person contact tracing where location data could be useful. We've heard it suggested, for example, that this data could be used to track future flare-ups of the virus by observing general patterns of people's movements in a given area. But even when transmission is less common, widespread testing may be more effective at containment, as may be happening in [South Korea](#).

4. Will health-based surveillance deter people from seeking health care? Already, there are reports that people subject to COVID-based location tracking are [altering their movements](#) to avoid embarrassing revelations. If a positive test result will lead to enhanced location surveillance, some people may avoid testing.

Conclusion

As our society struggles with COVID-19, far narrower “big data” surveillance proposals may emerge. Perhaps public health professionals will show that such proposals are necessary and proportionate. If so, EFF would seek safeguards, including mandatory expiration when the health crisis ends, independent supervision, strict anti-discrimination rules, auditing for efficacy and misuse, and due process for affected people.

But for now, government has not shown that new dragnet location surveillance powers would significantly help to contain COVID-19. It is the government's job

to show the public why this would work.

JOIN EFF LISTS

Join Our Newsletter!

Email updates on news, actions, events in your area, and more.

Email Address

Postal Code (optional)

Anti-spam question: Enter the three-letter abbreviation for Electronic Frontier Foundation:

SUBMIT



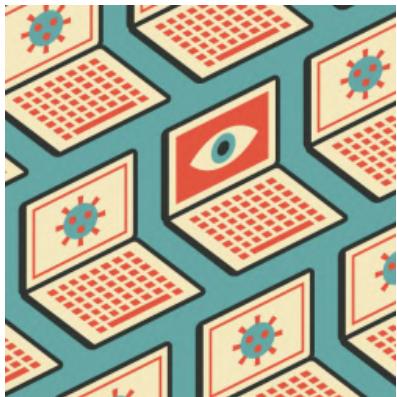
DEEPLINKS BLOG BY ERNESTO FALCON | MARCH 23, 2020

Social Distancing, The Digital Divide, and Fixing This Going Forward

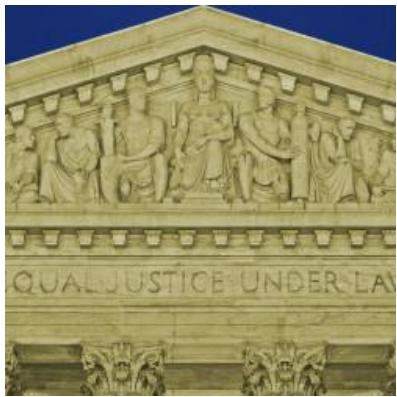
The California Public Records Act Is an



DEEPLINKS BLOG BY DAVE MAASS | MARCH 23, 2020
Essential Right, Even During a State of Emergency



DEEPLINKS BLOG BY CINDY COHN | MARCH 23, 2020
EFF and COVID-19: Protecting Openness, Security, and Civil Liberties



DEEPLINKS BLOG BY NAOMI GILENS, ALEX MOSS | MARCH 23, 2020
The Time Is Now: The Supreme Court Must Allow Live Cameras

Embracing Open Science in a Medical Crisis

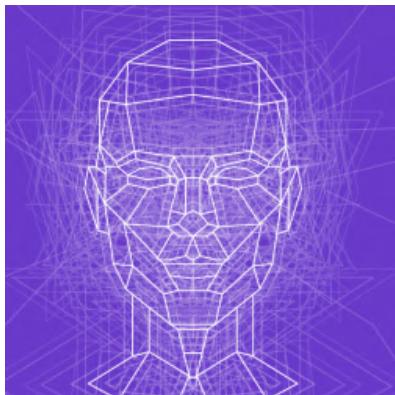


DEEPLINKS BLOG BY RORY MIR | MARCH 20, 2020



DEEPLINKS BLOG BY JASON KELLEY | MARCH 20, 2020

Governments Must Commit to Transparency During COVID-19 Crisis



DEEPLINKS BLOG BY MATTHEW GUARIGLIA | MARCH 19, 2020

Face Surveillance Is Not the Solution to the COVID-19 Crisis

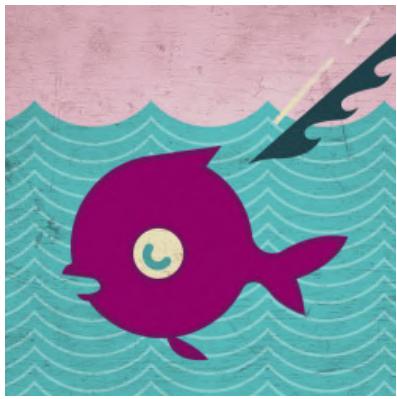
Right to Repair in Times of Pandemic



DEEPLINKS BLOG BY CORY DOCTOROW | MARCH 19, 2020



DEEPLINKS BLOG BY LINDSAY OLIVER | MARCH 19, 2020
What You Should Know About Online Tools During the COVID-19 Crisis



DEEPLINKS BLOG BY DALY BARNETT, SORAYA OKUDA |
MARCH 19, 2020
Phishing in the Time of COVID-19: How to Recognize Malicious Coronavirus Phishing Scams

ELECTRONIC FRONTIER FOUNDATION
eff.org
Creative Commons Attribution License

The California Consumer Privacy Act is effective as of January 1, 2020. California residents can learn more about their privacy rights here.

What kinds of information do we collect?

How do we use this information?

How is this information shared?

How do the Facebook Companies work together?

How can I manage or delete information about me?

How do we respond to legal requests or prevent harm?

How do we operate and transfer data as part of our global services?

How will we notify you of changes to this policy?

Privacy notice for California residents

How to contact Facebook with questions

Facebook Ads Controls

Privacy Basics

Cookies Policy

Terms

More Resources

- View a printable version of the Data Policy
- Interactive Tools
- Minors and Safety
- Facebook Privacy Page
- Facebook Safety Page
- Facebook Site Governance Page
- EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Notice

Data Policy

This policy describes the information we process to support Facebook, Instagram, Messenger and other products and features offered by Facebook ([Facebook Products](#) or Products). You can find additional tools and information in the [Facebook Settings](#) and [Instagram Settings](#).

[Return to top](#)

What kinds of information do we collect?

To provide the Facebook Products, we must process information about you. The types of information we collect depend on how you use our Products. You can learn how to access and delete information we collect by visiting the [Facebook Settings](#) and [Instagram Settings](#).

Things you and others do and provide.

- **Information and content you provide.** We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created. It can also include what you see through features we provide, such as our [camera](#), so we can do things like suggest masks and filters that you might like, or give you tips on using camera formats. Our systems automatically process content and communications you and others provide to analyze context and what's in them for the purposes described [below](#). Learn more about how you can control who can see the things you [share](#).
- Data with special protections: You can choose to provide information in your Facebook [profile fields](#) or Life Events about your religious views, political views, who you are “interested in,” or your health. This and other information (such as racial or ethnic origin, philosophical beliefs or trade union membership) could be subject to special protections under the laws of your country.
- **Networks and connections.** We collect information about the people, [Pages](#), accounts, [hashtags](#) and groups you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. We also collect contact information if you [choose to upload, sync or import it from a device](#) (such as an address book or call log or SMS log history), which we use for things like helping you and others find people you may know and for the other purposes listed [below](#).
- **Your usage.** We collect information about how you use our Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your

activities. For example, we log when you're using and have last used our Products, and what posts, videos and other content you view on our Products. We also collect information about how you use features like our camera.

- **Information about transactions made on our Products.** If you use our Products for purchases or other financial transactions (such as when you make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as your credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details.
- **Things others do and information they provide about you.** We also receive and analyze content, communications and information that other people provide when they use our Products. This can include information about you, such as when others share or comment on a photo of you, send a message to you, or upload, sync or import your contact information.

Device Information

As described below, we collect information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Products, and we combine this information across different devices you use. For example, we use information collected about your use of our Products on your phone to better personalize the content (including ads) or features you see when you use our Products on another device, such as your laptop or tablet, or to measure whether you took an action in response to an ad we showed you on your phone on a different device.

Information we obtain from these devices includes:

- **Device attributes:** information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
- **Device operations:** information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements (which can help distinguish humans from bots).
- **Identifiers:** unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts you use, and Family Device IDs (or other identifiers unique to Facebook Company Products associated with the same device or account).
- **Device signals:** Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
- **Data from device settings:** information you allow us to receive through device settings you turn on, such as access to your GPS location, camera or photos.
- **Network and connections:** information such as the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network, so we can do things like help you stream a video from your phone to your TV.
- **Cookie data:** data from cookies stored on your device, including cookie IDs and settings. Learn more about how we use cookies in the [Facebook Cookies Policy](#) and [Instagram Cookies Policy](#).

Information from partners.

Advertisers, app developers, and publishers can send us information through [Facebook Business Tools](#) they use, including our social plug-ins (such as the Like button), Facebook Login, our [APIs and SDKs](#), or the Facebook pixel. These partners provide information about your activities off Facebook—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have a Facebook account or are logged into Facebook. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.

Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. [Learn more](#) about the types of partners we receive data from.

To learn more about how we use cookies in connection with Facebook Business Tools, review the [Facebook Cookies Policy](#) and [Instagram Cookies Policy](#).

[Return to top](#)

How do we use this information?

We use the information we have (subject to choices you make) as described below and to provide and support the Facebook Products and related services described in the [Facebook Terms](#) and [Instagram Terms](#). Here's how:

Provide, personalize and improve our Products.

We use the information we have to deliver our Products, including to personalize features and content (including your [News Feed](#), [Instagram Feed](#), Instagram Stories and ads) and make suggestions for you (such as groups or [events](#) you may be interested in or topics you may want to follow) on and off our Products. To create personalized Products that are unique and relevant to you, we use your connections, preferences, interests and activities based on the data we collect and learn from you and others (including any [data with special protections](#) you choose to provide); how you use and interact with our Products; and the people, places, or things you're connected to and interested in on and off our Products. Learn more about how we use information about you to personalize your Facebook and Instagram experience, including features, content and recommendations in Facebook Products; you can also learn more about how we choose the [ads](#) that you see.

- **Information across Facebook Products and devices:** We connect information about your activities on different Facebook Products and devices to provide a more tailored and consistent experience on all Facebook Products you use, wherever you use them. For example, we can suggest that you join a group on Facebook that includes people you follow on Instagram or communicate with using Messenger. We can also make your experience more seamless, for example, by automatically filling in your registration information (such as your phone number) from one Facebook Product when you sign up for an account on a different Product.

Facebook

- **Location-related information:** We use [location-related information](#)-such as your current location, where you live, the places you like to go, and the businesses and people you're near-to provide, personalize and improve our Products, [including ads](#), for you and others. Location-related information can be based on things like precise device location (if you've allowed us to collect it), IP addresses, and information from your and others' use of Facebook Products (such as check-ins or events you attend).
- **Product research and development:** We use the information we have to develop, test and improve our Products, including by conducting surveys and research, and testing and troubleshooting new products and features.
- **Face recognition:** If you have it turned on, we use face recognition technology to recognize you in photos, videos and camera experiences. The face-recognition templates we create may constitute [data with special protections](#) under the laws of your country. Learn more about [how we use face recognition technology](#), or control our use of this technology in [Facebook Settings](#). If we introduce face-recognition technology to your Instagram experience, we will let you know first, and you will have control over whether we use this technology for you.
- **Ads and other sponsored content:** We use the information we have about you-including information about your interests, actions and connections-to select and personalize ads, offers and other sponsored content that we show you. Learn more about [how we select and personalize ads](#), and your choices over the data we use to select ads and other sponsored content for you in the [Facebook Settings](#) and [Instagram Settings](#).

Provide measurement, analytics, and other business services.

We use the information we have (including your activity off our Products, such as the websites you visit and ads you see) to help advertisers and other partners measure the effectiveness and distribution of their ads and services, and understand the types of people who use their services and how people interact with their websites, apps, and services. [Learn how we share information](#) with these partners.

Promote safety, integrity and security.

We use the information we have to verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, maintain the integrity of our Products, and promote safety and security on and off of Facebook Products. For example, we use data we have to investigate suspicious activity or violations of our terms or policies, or to [detect when someone needs help](#). To learn more, visit the [Facebook Security Help Center](#) and [Instagram Security Tips](#).

Communicate with you.

We use the information we have to send you marketing communications, communicate with you about our Products, and let you know about our policies and terms. We also use your information to respond to you when you contact us.

Research and innovate for social good.

We use the information we have (including from research partners we collaborate with) to conduct and support [research](#) and innovation on topics of general social welfare, technological advancement, public interest, health and well-being. For example, [we analyze information we have about migration patterns during crises](#) to aid relief efforts. [Learn more](#) about our research programs.

[Return to top](#)

How is this information shared?

Your information is shared with others in the following ways:

Sharing on Facebook Products

People and accounts you share and communicate with

When you share and communicate using our Products, you choose the audience for what you share. For example, when you post on Facebook, you select the audience for the post, such as a group, all of your friends, the public, or a customized list of people. Similarly, when you use Messenger or Instagram to communicate with people or businesses, those people and businesses can see the content you send. Your network can also see actions you have taken on our Products, including engagement with ads and sponsored content. We also let other accounts see who has viewed their Facebook or Instagram Stories.

Public information can be seen by anyone, on or off our Products, including if they don't have an account. This includes your Instagram username; any information you share with a public audience; information in your public profile on Facebook; and content you share on a Facebook Page, public Instagram account or any other public forum, such as Facebook Marketplace. You, other people using Facebook and Instagram, and we can provide access to or send public information to anyone on or off our Products, including in other Facebook Company Products, in search results, or through tools and APIs. Public information can also be seen, accessed, reshared or downloaded through third-party services such as search engines, APIs, and offline media such as TV, and by apps, websites and other services that integrate with our Products.

Learn more about what information is public and how to control your visibility on Facebook and Instagram.

Content others share or reshare about you

You should consider who you choose to share with, because people who can see your activity on our Products can choose to share it with others on and off our Products, including people and businesses outside the audience you shared with. For example, when you share a post or send a message to specific friends or accounts, they can download, screenshot, or reshare that content to others across or off our Products, in person or in virtual reality experiences such as Facebook Spaces. Also, when you comment on someone else's post or react to their content, your comment or reaction is visible to anyone who can see the other person's content, and that person can change the audience later.

People can also use our Products to create and share content about you with the audience they choose. For example, people can share a photo of you in a Story, mention or tag you at a location in a post, or share information about you in their posts or messages. If you are uncomfortable with what others have shared about you on our Products, you can learn how to report the content.

Information about your active status or presence on our Products.

People in your networks can see signals telling them whether you are

active on our Products, including whether you are currently active on [Instagram](#), [Messenger](#) or Facebook, or when you last used our Products.

Apps, websites, and third-party integrations on or using our Products.

When you choose to use third-party apps, websites, or other services that use, or are integrated with, our Products, they can receive information about what you post or share. For example, when you play a game with your Facebook friends or use a Facebook Comment or Share button on a website, the game developer or website can receive information about your activities in the game or receive a comment or link that you share from the website on Facebook. Also, when you download or use such third-party services, they can access your [public profile](#) on Facebook, and any information that you share with them. Apps and websites you use may receive your list of Facebook friends if you choose to share it with them. But apps and websites you use will not be able to receive any other information about your Facebook friends from you, or information about any of your Instagram followers (although your friends and followers may, of course, choose to share this information themselves). Information collected by these third-party services is subject to their own terms and policies, not this one.

Devices and operating systems providing native versions of Facebook and Instagram (i.e. where we have not developed our own first-party apps) will have access to all information you choose to share with them, including information your friends share with you, so they can provide our core functionality to you.

Note: We are in the process of restricting developers' data access even further to help prevent abuse. For example, we will remove developers' access to your Facebook and Instagram data if you haven't used their app in 3 months, and we are changing Login, so that in the next version, we will reduce the data that an app can request without app review to include only name, Instagram username and bio, profile photo and email address. Requesting any other data will require our approval.

New owner.

If the ownership or control of all or part of our Products or their assets changes, we may transfer your information to the new owner.

Sharing with Third-Party Partners

We work with third-party partners who help us provide and improve our Products or who use Facebook Business Tools to grow their businesses, which makes it possible to operate our companies and provide free services to people around the world. We don't sell any of your information to anyone, and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide. Here are the types of third parties we share information with:

Partners who use our analytics services.

We provide aggregated statistics and insights that help people and businesses understand how people are engaging with their posts, listings, Pages, videos and other content on and off the Facebook Products. For example, Page admins and Instagram business profiles receive information about the number of people or accounts who viewed, reacted to, or commented on their posts, as well as aggregate demographic and other information that helps them understand interactions with their Page or account.

Advertisers.

We provide advertisers with reports about the kinds of people seeing

their ads and how their ads are performing, but we don't share information that personally identifies you (information such as your name or email address that by itself can be used to contact you or identifies who you are) unless you give us permission. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We also confirm which Facebook ads led you to make a purchase or take an action with an advertiser.

Measurement partners.

We share information about you with companies that aggregate it to provide analytics and measurement reports to our partners.

Partners offering goods and services in our Products.

When you subscribe to receive premium content, or buy something from a seller in our Products, the content creator or seller can receive your public information and other information you share with them, as well as the information needed to complete the transaction, including shipping and contact details.

Vendors and service providers.

We provide information and content to vendors and service providers who support our business, such as by providing technical infrastructure services, analyzing how our Products are used, providing customer service, facilitating payments or conducting surveys.

Researchers and academics.

We also provide information and content to research partners and academics to conduct research that advances scholarship and innovation that support our business or mission, and enhances discovery and innovation on topics of general social welfare, technological advancement, public interest, health and well-being.

Law enforcement or legal requests.

We share information with law enforcement or in response to legal requests in the circumstances outlined below.

Learn more about how you can control the information about you that you or others share with third-party partners in the [Facebook Settings](#) and [Instagram Settings](#).

[Return to top](#)

How do the Facebook Companies work together?

Facebook and Instagram share infrastructure, systems and technology with other Facebook Companies (which include WhatsApp and Oculus) to provide an innovative, relevant, consistent and safe experience across all Facebook Company Products you use. We also process information about you across the Facebook Companies for these purposes, as permitted by applicable law and in accordance with their terms and policies. For example, we process information from WhatsApp about accounts sending spam on its service so we can take appropriate action against those accounts on Facebook, Instagram or Messenger. We also work to understand how people use and interact with Facebook Company Products, such as understanding the number of unique users on different Facebook Company Products.

[Return to top](#)

How can I manage or delete information about me?

We provide you with the ability to access, rectify, port and erase your data. Learn more in your [Facebook Settings](#) and [Instagram Settings](#).

We store data until it is no longer necessary to provide our services and Facebook Products, or until your account is deleted - whichever comes first. This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, when you search for something on Facebook, you can access and delete that query from within your search history at any time, but the log of that search is deleted after 6 months. If you submit a copy of your government-issued ID for account verification purposes, we delete that copy 30 days after review, unless otherwise stated. Learn more about deletion of [content you have shared](#) and [cookie data obtained through social plugins](#).

When you delete your account, we [delete things](#) you have posted, such as your photos and status updates, and you won't be able to recover that information later. Information that others have shared about you isn't part of your account and won't be deleted. If you don't want to delete your account but want to temporarily stop using the Products, you can deactivate your account instead. To delete your account at any time, please visit the [Facebook Settings](#) and [Instagram Settings](#).

[Return to top](#)

How do we respond to legal requests or prevent harm?

We access, preserve and share your information with regulators, law enforcement or others:

- In response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States when we have a good-faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.
- When we have a good-faith belief it is necessary to: detect, prevent and address fraud, unauthorized use of the Products, violations of our terms or policies, or other harmful or illegal activity; to protect ourselves (including our rights, property or Products), you or others, including as part of investigations or regulatory inquiries; or to prevent death or imminent bodily harm. For example, if relevant, we provide information to and receive information from third-party partners about the reliability of your account to prevent fraud, abuse and other harmful activity on and off our Products.

Information we receive about you (including financial transaction data related to purchases made with Facebook) can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or

investigations of possible violations of our terms or policies, or otherwise to prevent harm. We also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

[Return to top](#)

How do we operate and transfer data as part of our global services?

We share information globally, both internally within the Facebook Companies, and externally with our partners and with those you connect and share with around the world in accordance with this policy. Your information may, for example, be transferred or transmitted to, or stored and processed in the United States or other countries outside of where you live for the purposes as described in this policy. These data transfers are necessary to provide the services set forth in the [Facebook Terms](#) and [Instagram Terms](#) and to globally operate and provide our Products to you. We utilize [standard contract clauses](#), rely on the European Commission's [adequacy decisions](#) about certain countries, as applicable, and obtain your consent for these data transfers to the United States and other countries.

[Return to top](#)

How will we notify you of changes to this policy?

We'll notify you before we make changes to this policy and give you the opportunity to review the revised policy before you choose to continue using our Products.

[Return to top](#)

Privacy notice for California residents

If you are a California resident, you can learn more about your consumer privacy rights by reviewing the [California Privacy Notice](#).

[Return to top](#)

How to contact Facebook with questions

You can learn more about how privacy works [on Facebook](#) and [on Instagram](#). If you have questions about this policy, you can contact us as described below.

Contact Us

You can contact us [online](#) or by mail at:

Facebook, Inc.
ATTN: Privacy Operations
1601 Willow Road
Menlo Park, CA 94025

Date of Last Revision: January 11, 2021

[About](#) [Create Ad](#) [Create Page](#) [Developers](#) [Careers](#) [Privacy](#) [Cookies](#) [Ad Choices](#) [Terms](#) [Help](#)

Facebook © 2021

English (US) [Español](#) [Français \(France\)](#) [中文\(简体\)](#) [العربية](#) [Português \(Brasil\)](#) [한국어](#) [Italiano](#) [Deutsch](#) [हिन्दी](#) [日本語](#)

**GLOBAL RELIEF FOUNDATION,
INC., Plaintiff,**

v.

**Paul H. O'NEILL, Colin L. Powell, John
Ashcroft, R. Richard Newcomb, and
Robert S. Mueller, III, Defendants.**

No. 02 C 674.

United States District Court,
N.D. Illinois,
Eastern Division.

June 11, 2002.

***MEMORANDUM OPINION
AND ORDER***

ANDERSEN, District Judge.

This case is before the Court on the motion of plaintiff Global Relief Foundation, Inc. for preliminary injunctive relief pursuant to Federal Rule of Civil Procedure 65. For the following reasons, the motion is denied.

OVERVIEW

Before addressing the motion for preliminary injunction filed by the plaintiff, Global Relief Foundation ("Global Relief"), a brief description of this case is in order.

On December 14, 2001, the Federal Bureau of Investigation ("FBI") searched the headquarters of Global Relief and the home of its executive director. Pursuant to the searches, materials were seized for analysis by the FBI. Global Relief contends that both the search and seizure were unauthorized by law and unconstitu-

tional. The defendants maintain that both the search and seizure were lawfully authorized by the Foreign Intelligence Surveillance Act and that they were constitutional. This Court agrees with the defendants.

Also on December 14, 2001, the Office of Foreign Asset Control ("OFAC") of the United States Department of the Treasury issued a blocking order freezing the financial assets of Global Relief pending the FBI's investigation of what relationship, if any, Global Relief might have to the terrorists behind the September 11, 2001 attacks on the World Trade Center and the Pentagon. Global Relief contends that the order temporarily "freezing" its assets was not authorized by statute, executive order or the Constitution. The defendants maintain that this blocking order was both lawful and constitutional. They cite the International Emergency Economic Powers Act, as amended by the USA Patriot Act, as the statutory basis for the authority to issue the blocking order. This authority was granted first to the President and then delegated by him to the Treasury pursuant to Executive Order Number 13224. Once again, this Court agrees with the defendants.

The assets seized for analysis and the funds blocked by OFAC's order have been seized and blocked "pending investigation" of Global Relief and others. Thus far, no agency of the United States government has declared or requested any forfeiture of assets to the government. Nor have any individuals or Global Relief been charged with any crimes. Hence, Global Relief's request for a preliminary injunction is directed only to the release of funds and materials seized for investigative purposes while the investigation itself is ongoing.

To justify its emergency search and, to some extent, the blocking order, defendants have asked this Court to review materials, *in camera* and *ex parte*, without

revealing them to Global Relief or its attorneys. In accordance with our order of April 5, 2002, we have reviewed materials furnished by the FBI to us and have concluded that they are relevant to the ongoing investigation and that their disclosure to Global Relief, while the investigation is pending, could undermine this investigation and others of national significance.

BACKGROUND

Global Relief began operating in 1992 as a domestic, non-profit corporation chartered and headquartered in Illinois. According to its complaint, Global Relief claims to be a charitable organization that funds humanitarian relief programs throughout the world. These programs allegedly distribute food, fund schools for orphans, and provide medical services.

Global Relief characterizes itself as the largest U.S.-based Islamic charitable organization "with respect to the geographic scope of its relief programs." (Complaint ¶ 12.) As contributions to Global Relief increased (in 1995, the organization reported accepting donations totaling \$431,155; by 2000, it reported nearly \$3.7 million), it appears to have expanded the reach of its efforts. In 1995, it reported funding programs in Chechnya, Bosnia, Pakistan, Kashmir, and Lebanon. It reported funding additional programs in Afghanistan and Azerbaijan in 1996, Bangladesh in 1997, Iraq and Somalia in 1998, Albania, Belgium, China, Eritrea, Kosovo, and Turkey in 1999, and, eventually, Ethiopia, Jordan, Palestine, and Sierra Leone in 2000. Global Relief also has funded programs in Gaza and the West Bank. (Complaint ¶ 11.) To assist with the distribution of humanitarian aid abroad, Global Relief established regional offices in Belgium, Azerbaijan, and Pakistan. Reportedly, such offices received hundreds of thousands of dollars in contributions, in addition to the amounts

reported by the headquarters in the United States. Although Global Relief has funded relief programs in the United States, over 90 percent of its donations have been sent abroad.

On September 11, 2001, terrorists attacked the United States. Individuals hijacked four commercial airliners containing passengers and crew and flew them deliberately into the two towers of the World Trade Center in New York City as well as into the Pentagon near Washington, D.C. The fourth plane was diverted from its path and crashed in rural Pennsylvania. Over 3,000 people were murdered.

On September 24, 2001, President George W. Bush declared a national emergency with respect to the "grave acts of terrorism and threats of terrorism . . . and the continuing and immediate threat of further attacks on United States nationals or the United States." Exec. Order No. 13224, 66 Fed.Reg. 49074 (2001). The President determined that the acts perpetrated on September 11 constituted "an unusual and extraordinary threat to national security, foreign policy, and economy of the United States." In light of the "pervasiveness and expansiveness of the financial foundation of terrorists," the President cited the need for financial sanctions against individuals or organizations that engage in or support terrorism throughout the world.

On December 14, 2001, pursuant to the Foreign Intelligence Surveillance Act, then-acting Deputy Attorney General Larry D. Thompson authorized the search of Global Relief's Bridgeview, Illinois office and the residence of its executive director. The FBI's Chicago Division Joint Terrorism Task Force conducted both searches. From the Global Relief office, the FBI seized items including computers and servers, modems, a cellular phone, hand-held radios, video and audio tapes, cassette

tapes, computer diskettes, a credit card imprinter, foreign currency, U.S. mail, photographs, receipts, documents, and records. From the executive director's residence, the FBI seized computers, computer diskettes, video and audio tapes, cassette tapes, date books, a cellular telephone, a camera, a palm pilot, credit cards, foreign currency, photographs, documents, records, and \$13,030 in U.S. currency. Since being seized, the items removed from both the Global Relief office and the executive director's residence have been secured in FBI custody for review and analysis.

Also, on December 14, 2001, pursuant to the International Emergency Economic Powers Act and President Bush's Executive Order, OFAC issued a "Blocking Notice and Requirement to Furnish Information" to Global Relief, which "froze," until further notice, the funds, accounts, and business records in which the organization had an interest. OFAC has claimed that it acted on the basis of substantial classified and unclassified information related to Global Relief's possible connections with terrorist organizations.

The blocking order advised Global Relief of the administrative procedures available to it should it choose to contest OFAC's action, including the right to challenge the blocking and to seek licenses to resume operations in whole or in part. Although Global Relief applied for and was granted licenses to access limited blocked funds to pay for legal expenses, salaries, payroll taxes, health insurance, rent, and utilities, it did not challenge the blocking order itself through administrative procedures.

On January 28, 2002, Global Relief filed a petition for declaratory judgment and injunctive relief and for a writ of mandamus with this Court, naming Paul H. O'Neill, Colin L. Powell, John Ashcroft, R. Richard Newcomb, and Robert S. Mueller,

III, in their official capacities, as defendants (collectively, the "defendants"). In its petition, Global Relief requested that the defendants be ordered to "unfreeze" its assets and return the items seized during the search of the organization's office and the executive director's residence. In addition, on February 12, 2002, Global Relief filed a motion for preliminary injunction, arguing that the blocking of its assets and records was both unlawful and unconstitutional.

1. *The Foreign Intelligence Surveillance Act*

As the first part of its statutory argument offered in support of its motion for a preliminary injunction, Global Relief contends that the search of its headquarters and the subsequent search of the home of Global Relief's executive director was an *ultra vires* action (which is defined as an act which is beyond the powers conferred on executive agencies by Congress). In response to this argument, the defendants have asserted that the searches conducted on December 14, 2001 were in accordance with the procedures identified in the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, (hereinafter "FISA").

FISA was passed by Congress in 1978 to "put to rest a troubling constitutional issue" regarding the President's "inherent power to conduct warrantless electronic surveillance in order to gather foreign intelligence in the interests of national security." *U.S. v. Squillacote*, 221 F.3d 542, 552 (4th Cir.2000) (citing *ACLU Found. of S. California v. Barr*, 952 F.2d 457, 460 (D.C.Cir.1991)). FISA was enacted to create by statute a "secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights." S.Rep. No. 95-604, at 15 (1978), reprinted in 1978 U.S.C.C.A.N. 3904, 3916.

To oversee the exercise of the powers granted by FISA to the Executive Branch and to ensure that the new investigatory

power is used constitutionally and lawfully, FISA established the Foreign Intelligence Surveillance Court, which is composed of seven federal district court judges appointed by the Chief Justice of the United States, to review applications for authorization of electronic surveillance aimed at obtaining intelligence information. *See* 50 U.S.C. § 1803. In 1994, FISA was amended to give the Foreign Intelligence Surveillance Court jurisdiction to hear applications for physical searches as well as electronic searches. *See* 50 U.S.C. § 1821–29. Each application to the Foreign Intelligence Surveillance Court must first be personally approved by the Attorney General. *See* 50 U.S.C. § 1804(a). The application must contain, among other things, a statement of facts to justify the belief that the target of the search is a foreign power or an agent of a foreign power, that the premises or property to be searched contains foreign intelligence information, and that the premises or property to be searched is owned, used, or possessed by a foreign power or an agent of a foreign power. Additionally, the application must contain a certification by a senior Executive Branch official that the information sought is foreign intelligence information which could not reasonably be obtained by normal investigative techniques. *See* 50 U.S.C. § 1823(a).

When the target of the surveillance is a “United States person” (which the parties concede Global Relief is), the Foreign Intelligence Surveillance Court may issue an order authorizing the surveillance only if a FISA judge concludes there is “probable cause” to believe that the target of the surveillance is a foreign power or agent of a foreign power, that proposed “minimization procedures” are sufficient under the terms of the statute, that the certifications required by section 1823 have been made, and that the certifications are not “clearly erroneous.” 50 U.S.C. § 1824(a)(3)–(5). Under the statute, an agent of a foreign

power is any person “who knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States.” 50 U.S.C. § 1801(b)(2)(A). FISA authorizes the federal district courts to review warrant applications and probable cause determinations made by the Foreign Intelligence Surveillance Court. *See* 50 U.S.C. § 1825(d)–(g).

Furthermore, FISA provides that, when the United States intends to use in a district court information derived from a FISA search or when an aggrieved party requests discovery of information related to a FISA application, the Attorney General must file “an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States.” 50 U.S.C. § 1825(g). Attorney General John Ashcroft has filed such an affidavit in this case. This having been done, the statute requires us to “review *in camera* and *ex parte* the application, order, and such other materials relating to the physical search as may be necessary to determine whether the physical search of the aggrieved party was lawfully authorized and conducted.” *Id.* As we noted in our April 5, 2002 ruling denying Global Relief’s motion to prevent consideration of certain materials *in camera* and *ex parte*, see *Global Relief Foundation, Inc. v. O’Neill*, 205 F.Supp.2d 885, 887–88 (N.D. Ill. 2002), this Court decided to consider these submissions. We have done so on an *ex parte* basis and have not permitted counsel for Global Relief to review the submissions with us.

With this analytical framework in mind, we now turn to the facts of the case currently before us. As was discussed above, agents of the FBI arrived at the corporate headquarters of Global Relief and the

home of its executive director on December 14, 2001 and seized a considerable amount of material they felt was relevant to their investigation of Global Relief's activities. As the defendants have conceded in their briefs, no warrant had been obtained before the FBI arrived either at Global Relief's headquarters or the executive director's residence. Nevertheless, FISA includes a provision which states that, when the Attorney General declares that "an emergency situation exists with respect to the execution of a search to obtain foreign intelligence information" prior to the Foreign Intelligence Surveillance Court acting on the application, a warrantless search is authorized. 50 U.S.C. § 1824(e)(1)(B)(i). When such an emergency situation arises, the government must submit a warrant application to the Foreign Intelligence Surveillance Court within 72 hours of the warrantless search for approval. See 50 U.S.C. § 1824(e), as amended by, P.L. 107-108, 115 Stat. 1394, 1402 (2001). In this case, the failure of the FBI agents to present a FISA warrant on December 14 was caused by the Assistant Attorney General's declaration that an emergency situation existed with respect to the targeted documents and material. The defendants did submit a warrant application to the Foreign Intelligence Surveillance Court on December 15, as required by 50 U.S.C. § 1824(e). We have reviewed the warrant that issued and the submissions to the Foreign Intelligence Surveillance Court in support of that warrant.

[3] We conclude that the FISA application established probable cause to believe that Global Relief and the executive director were agents of a foreign power, as that term is defined for FISA purposes, at the time the search was conducted and the application was granted. We are also satisfied that Global Relief and the executive director were not targeted because of any protected First Amendment activities in

which they may have engaged. Given the sensitive nature of the information upon which we have relied in making this determination and the Attorney General's sworn assertion that disclosure of the underlying information would harm national security, it would be improper for us to elaborate further on this subject. See *Squillacote*, 221 F.3d at 554 (finding probable cause to authorize FISA surveillance and declining to comment further on the probable cause issue when the Attorney General filed an affidavit); *United States v. Isa*, 923 F.2d 1300, 1304 (8th Cir.1991) (same).

This Court has concluded that disclosure of the information we have reviewed could substantially undermine ongoing investigations required to apprehend the conspirators behind the September 11 murders and undermine the ability of law enforcement agencies to reduce the possibility of terrorist crimes in the future. Furthermore, this Court is persuaded that the search and seizure made by the FBI on December 14 were authorized by FISA. Accordingly, we decline plaintiff's request that we declare the search invalid and order the immediate return of all items seized.

Amendment provides that “the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated; and no warrant shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

We reject Global Relief’s argument because FISA’s safeguards provide sufficient protection for the rights guaranteed by the Fourth Amendment in the context of foreign intelligence activities. We agree with the many courts which have held that searches conducted pursuant to FISA do not violate the protections afforded by the Fourth Amendment. *See, e.g., United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir.1987); *United States v. Cavanagh*, 807 F.2d 787, 790–92 (9th Cir.1987); *United States v. Duggan*, 743 F.2d 59, 73 (2d Cir.1984).

For these reasons it is unlikely that Global Relief will succeed in proving a violation of the Fourth Amendment.

9. *Fourth Amendment*

[23] Global Relief next argues that defendants unconstitutionally searched its offices and seized its property in violation of the Fourth Amendment. The Fourth

NOTE

WHY THE UNITED STATES SUPREME COURT'S RULING IN KYLLO v. UNITED STATES¹ IS NOT THE FINAL WORD ON THE CONSTITUTIONALITY OF THERMAL IMAGING

In 1991 Agent William Elliott of the United States Department of Interior began to suspect that Danny Kyllo was using his home for the indoor cultivation of marijuana.² This suspicion arose out of findings gleaned by a joint task force organized to investigate a possible marijuana production and distribution ring.³ The initial investigation centered on Sam Shook, the father of Kyllo's neighbor.⁴ After discovering information that suggested Kyllo's involvement in the growing and distribution of marijuana, Agent Elliott contacted Oregon state law enforcement officers who provided him with additional information that strengthened the suspicions against Kyllo.⁵ Agent Elliot subpoe-

1. *Kyllo v. United States*, 533 U.S. 27, 121 S. Ct. 2038 (2001).

2. *Id.* at 2041.

3. *United States v. Kyllo*, 809 F. Supp. 787, 789 (D. Or. 1992), *aff'd in part*, *United States v. Kyllo*, 26 F.3d 134 (9th Cir. 1994), *opinion superseded*, *United States v. Kyllo*, 37 F.3d 526 (9th Cir. 1994), *rev'd*, *United States v. Kyllo*, 140 F.3d 1249 (9th Cir. 1998), *opinion withdrawn*, *United States v. Kyllo*, 184 F.3d 1059 (9th Cir. 1999), *opinion superseded*, *United States v. Kyllo*, 190 F.3d 1041 (9th Cir. 1999), *cert. granted*, *Kyllo v. United States*, 530 U.S. 1305 (2000), *rev'd*, *Kyllo v. United States*, 121 S. Ct. 2038 (2001). The joint task force was comprised of the United States Department of Interior, the Bureau of Land Management, the Tillamook County Sheriff's Department, and the Oregon State Police Bureau.

4. See *id.* The investigation of Sam Shook eventually began to focus on Tova Shook who resided at 890 Rhododendron Drive, Florence Oregon. Kyllo resided at 878 Rhododendron Drive.

5. *United States v. Kyllo*, 140 F.3d 1249, 1250-51 (9th Cir. 1998), *opinion withdrawn*, *United States v. Kyllo*, 184 F.3d 1059 (9th Cir. 1999), *opinion superseded*, *United States v. Kyllo*, 190 F.3d 1041 (9th Cir. 1999), *cert. granted*, *Kyllo v. United States*, 530 U.S. 1305 (2000), *rev'd*, *Kyllo v. United States*, 121 S. Ct. 2038 (2001). The information included that: Kyllo lived with his wife, Luanne, in one unit of a triplex in Florence Oregon, the triplex was also occupied by others who were suspects in the drug investigation, Kyllo allegedly told a police informant that he and Luanne could supply the informant with marijuana, and the previous month, Luanne had been arrested for delivery and possession of a controlled substance.

naed Kyllo's utility records and compared the use of electricity in Kyllo's triplex with a chart developed by the Portland General Electric Company.⁶ That chart serves as a guide for estimating average power usage relative to square footage, type of heating and accessories, and the number of people living in the residence.⁷ Based upon the comparisons between average electrical usage and Kyllo's utility records, Elliott concluded that Kyllo's use was abnormally high, a common indicator of indoor marijuana cultivation.⁸ In order to determine if heat was emanating from Kyllo's home in levels consistent with the use of high intensity bulbs required for indoor growth, Elliott requested Staff Sergeant Daniel Haas of the Oregon National Guard to examine the triplex with an Agema Thermovision 210 thermal imaging device.⁹ The scan was conducted from the passenger seat of Elliott's vehicle from across the street in front of Kyllo's house as well as from the street behind the house.¹⁰ The scan showed that the roof over the garage and a side wall of petitioner's home radiated more heat than the rest of the home and were substantially warmer than the neighboring homes of the triplex.¹¹ Elliott and Haas concluded that the emanating heat indicated Kyllo was using halide lights to grow marijuana in his house.¹² Based upon the thermal imaging, utility bills, and tips from informants, Elliot was able to obtain a warrant authorizing the search of petitioner's home.¹³ The search led to the discovery of an indoor growing operation involving more than 100 marijuana plants.¹⁴ Kyllo's motion to

6. United States v. Kyllo, 809 F. Supp. 787, 790 (D. Or. 1992), *aff'd in part*, United States v. Kyllo, 26 F.3d 134 (9th Cir. 1994), *opinion superseded*, United States v. Kyllo, 37 F.3d 526 (9th Cir. 1994), *rev'd*, United States v. Kyllo, 140 F.3d 1249 (9th Cir. 1998), *opinion withdrawn*, United States v. Kyllo, 184 F.3d 1059 (9th Cir. 1999), *opinion superseded*, United States v. Kyllo, 190 F.3d 1041 (9th Cir. 1999), *cert. granted*, Kyllo v. United States, 530 U.S. 1305 (2000), *rev'd*, Kyllo v. United States, 121 S. Ct. 2038 (2001).

7. *Id.* at 790.

8. See United States v. Pinson, 24 F.3d 1056, 1057 (8th Cir. 1994). Indoor marijuana growth is dependent upon high intensity light bulbs that use between four hundred and one thousand-watt bulbs. Use of high intensity bulbs will result in greater electricity use.

9. United States v. Kyllo, 140 F.3d 1249, 1251 (9th Cir. 1998), *opinion withdrawn*, United States v. Kyllo, 184 F.3d 1059 (9th Cir. 1999), *opinion superseded*, United States v. Kyllo, 190 F.3d 1041 (9th Cir. 1999), *cert. granted*, Kyllo v. United States, 530 U.S. 1305 (2000), *rev'd*, Kyllo v. United States, 121 S. Ct. 2038 (2001).

10. Kyllo v. United States, 121 S. Ct. 2038, 2041 (2001).

11. *Id.*

12. *Id.*

13. *Id.*

14. *Id.*

suppress the seized evidence was denied, and thereafter he entered a conditional guilty plea.¹⁵

After a tangled procedural history, bouncing back and forth between the Federal District Court in Oregon and the Ninth Circuit Court of Appeals,¹⁶ the United Supreme Court granted certiorari in September 2000¹⁷ more than eight years after the thermal image scan had been conducted on Kyllo's triplex.¹⁸

WHAT IS A THERMAL IMAGER?

Before examining thermal imaging and its impact upon the Fourth Amendment, a brief synopsis of the technology is needed to better understand the constitutional implications. Objects with a temperature above absolute zero emit infrared radiation; the hotter an object becomes, the more infrared radiation is emitted.¹⁹ The emitted radiation is not visible to the human eye because infrared energy occurs at a rate one thousand times slower than visible light.²⁰ A thermal imager detects infrared emissions, and then converts the heat readings into a two-dimensional picture, typically black and white.²¹ The picture depicts various shades of gray according to how much radiation the object releases.²² Hotter objects are lighter in color due to the fact they radiate more infrared energy, while the cooler objects

15. *Id.*

16. *United States v. Kyllo*, 809 F. Supp. 787, 790 (D. Or. 1992), *aff'd in part*, *United States v. Kyllo*, 26 F.3d 134 (9th Cir. 1994), *opinion superseded*, *United States v. Kyllo*, 37 F.3d 526 (9th Cir. 1994), *rev'd*, *United States v. Kyllo*, 140 F.3d 1249 (9th Cir. 1998), *opinion withdrawn*, *United States v. Kyllo*, 184 F.3d 1059 (9th Cir. 1999), *opinion superseded*, *United States v. Kyllo*, 190 F.3d 1041 (9th Cir. 1999), *cert. granted*, *Kyllo v. United States*, 530 U.S. 1305 (2000), *rev'd*, *Kyllo v. United States*, 121 S. Ct. 2038 (2001).

17. See *Kyllo v. United States*, 530 U.S. 1305 (2000).

18. *United States v. Kyllo*, 809 F. Supp. 787 (D. Or. 1992), *aff'd in part*, *United States v. Kyllo*, 26 F.3d 134 (9th Cir. 1994), *opinion superseded*, *United States v. Kyllo*, 37 F.3d 526 (9th Cir. 1994), *rev'd*, *United States v. Kyllo*, 140 F.3d 1249 (9th Cir. 1998), *opinion withdrawn*, *United States v. Kyllo*, 184 F.3d 1059 (9th Cir. 1999), *opinion superseded*, *United States v. Kyllo*, 190 F.3d 1041 (9th Cir. 1999), *cert. granted*, *Kyllo v. United States*, 530 U.S. 1305 (2000), *rev'd*, *Kyllo v. United States*, 121 S. Ct. 2038 (2001).

19. Thomas D. Colbridge, *Thermal Imaging: Much Heat but Little Light*, *FBI Law Enforcement Bull.*, Dec. 1997, at 18.

20. Mindy G. Wilson, Note, *The Prewarrant Use of Thermal Imagery: Has This Technological Advance in the War Against Drugs Come at the Expense of Fourth Amendment Protections Against Unreasonable Searches?*, 83 Ky. L.J. 891, 892 (1995).

21. See Colbridge, *supra* note 19, at 18.

22. *Id.*

appear darker.²³ A thermal imager is not capable of measuring the actual temperature of the environment, but detects temperature differentials between the objects and the air temperature.²⁴ A thermal imaging device does not transmit rays or beams that can penetrate the home; instead it passively scans thermal energy that is radiated from the home.²⁵

The United States Army first developed the thermal imager to assist soldiers in locating enemies during combat.²⁶ Today, thermal imagers serve numerous functions that include finding missing persons, detecting "hot spots" in forest fires hidden by smoke, identifying inefficient insulation, detecting overloaded powerlines,²⁷ assisting in fugitive apprehensions and detecting illegal border crossings.²⁸

As law enforcement officials throughout the United States have cracked down on the drug problem which plagues the nation, those who previously had grown marijuana outdoors turned to indoor cultivation where the risk of detection was significantly lower. Thermal imagers have therefore recently been employed by law enforcement agencies in the war on drugs to detect excess heat emanating from private residences - a common indicator of an indoor marijuana farm.²⁹ The high intensity bulbs used for indoor cultivation produce heat of 150 degrees or more Fahrenheit.³⁰ However, the optimal growing temperature for marijuana plants is between 68 and 72 degrees Fahrenheit.³¹ Therefore this excess heat must be vented from indoors in order to maintain ideal growing conditions; the necessity of venting excess heat works to the advantage of law enforcement officials who could scan the suspect's home to determine if emissions were indicative of indoor marijuana operations.³² The two interests at battle in

23. *Id.*

24. *Id.*

25. Wilson, *supra* note 20, at 897.

26. Matt Greenberg, Casenote, *Warrantless Thermal Imaging May Impermissibly Invade Home Privacy: United States v. Kyllo*, 140 F.3d 1249 (9th Cir. 1998), Withdrawn, 1999 WL 548267 (9th Cir. 1999), Superseded on Rehearing by 1999 WL 694733 (9th Cir. 1999), 68 U. Cin. L. Rev. 151, 155 (1999).

27. Doyle Baker, Feature, *More Heat than Light: Judicial Discord Regarding Thermal Heat and Imagery and the Fourth Amendment*, 32-FEB Prosecutor 16, (1998).

28. Colbridge, *supra* note 19, at 19.

29. *Id.*

30. United States v. Pinson, 24 F.3d 1056, 1057 (8th Cir. 1994).

31. *Id.* at 1057.

32. *See id.*

the thermal imaging cases are the government's war on drugs and concerns for American civil liberties.³³

FOURTH AMENDMENT GUARANTEES

The Fourth Amendment of the United States Constitution guarantees citizens their privacy will not be unreasonably invaded by providing:

(t)he right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.³⁴

The basic purpose of the Fourth Amendment is to safeguard the privacy and security of individuals against arbitrary invasion by the government.³⁵

The Constitution does not prohibit all searches or seizures, but only those that are unreasonable.³⁶ A search is reasonable when conducted according to the warrant requirement of the Fourth Amendment.³⁷ "The warrant procedure is designed to guarantee that a decision to search private property is justified by a reasonable government interest."³⁸ The determination of reasonableness is based upon a balancing test, weighing the need for government search or seizure against the individual right to privacy as guaranteed by the Fourth Amendment.³⁹ The balancing test to determine when the right of privacy must yield to the right of search is to be determined by a judicial officer, not a police officer or government agent.⁴⁰ The need for the judgment by a judicial officer to be interposed between the citizen and the police is to ensure a neutral drawing of inferences from the evidence, as opposed to a drawing of inferences by a law enforcement officer who is "engaged in the often competitive enterprise of ferreting out crime."⁴¹ If upon weighing the evidence the neutral judicial officer decides there is a valid public interest that justifies the intrusion, then there exists probable cause to issue a search warrant limited to the

33. Joan Biskupic, *Justices Rule for Privacy*, USA Today, June 12, 2001, at 10A.

34. U.S. CONST. amend. IV.

35. *Camara v. Municipal Court*, 387 U.S. 523, 528 (1967).

36. *Carroll v. United States*, 267 U.S. 132 (1925).

37. See *Camara*, 387 U.S. 523.

38. *Id.* at 539.

39. *Terry v. Ohio*, 392 U.S. 1, 21 (1968).

40. *Johnson v. United States*, 333 U.S. 10, 14 (1948).

41. *Id.*

necessary scope of investigation.⁴² Searches conducted outside the prescribed judicial process, without prior approval, are *per se* unreasonable and therefore unconstitutional, unless within one of the limited exceptions.⁴³

All evidence obtained by searches and seizures in violation of the Fourth Amendment is inadmissible against the defendant based upon the exclusionary principle.⁴⁴ The Fourth Amendment protections against arbitrary government intrusion do not extend to conduct that is not considered a search or seizure.⁴⁵ Therefore, whether government conduct is classified as a search or seizure is the pivotal question in Fourth Amendment analysis; if there is no search or seizure, there is not a constitutional question.

42. *Camara*, 387 U.S. at 539.

43. *Katz v. United States*, 389 U.S. 347 (1967). Exceptions to the warrant requirement include: searches incidental to arrest, during hot pursuit, conducted with consent of the suspect, and possibly searches for national security reasons. *Katz*, 389 U.S. at 358 nn.20-23.

44. *Mapp v. Ohio*, 367 U.S. 643, 655 (1961).

45. Baker, *supra* note 27, at 16.

THE SUPREME COURT'S RULING ON THERMAL IMAGING

In what has been characterized as an unusual alignment of justices, in a 5-4 ruling the United States Supreme Court, majority opinion written by Justice Anton Scalia,¹⁰⁷ held "where . . . the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment 'search', and is presumptively unreasonable without a warrant."¹⁰⁸

The Court began its analysis by focusing on the guarantees of privacy and the emphasis placed by the Fourth Amendment on the home, stating that "[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."¹⁰⁹ With few exceptions, the warrantless search of a home is unreasonable.¹¹⁰ The Court goes on to note that this case is not a simple one under the existing precedent, due to the fact that well into the twentieth century, Fourth Amendment analysis was tied to common law trespass.¹¹¹ The majority explains that the question the Court must confront is "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."¹¹²

The majority rejected the distinction between "off-the-wall" observations and "through-the-wall" surveillance.¹¹³ The dissent argues that there should be a differentiation between scans that simply detect emitted heat, referred to as "off-the wall," and scans that can detect

107. Edward Walsh, *High-Tech Devices Require a Warrant*, The Washington Post, June 12, 2001, at A1. The majority opinion included Justices Scalia, Thomas, Souter, Ginsburg, and Breyer.

108. *Kyllo*, 121 S. Ct. at 2046.

109. *Id.* at 2041 (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961)).

110. *Id.* at 2042.

111. *Id.*

112. *Id.* at 2043.

113. *Id.* at 2044.

activity within the house, “through-the-wall.”¹¹⁴ The dissent states that a scan determined to be “through-the-wall” should be found to constitute an unreasonable search in violation of the Fourth Amendment; while a finding of “off-the-wall” imaging should be considered reasonable without the issuing of a warrant.¹¹⁵ The majority compares the argument that the thermal imager detected only radiated heat from external surfaces with the fact that a microphone placed outside the house would pick up only sound emanating from within.¹¹⁶ The Court found that such a mechanical interpretation had been rejected in *Katz*.¹¹⁷ The Court stated:

[r]evering that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home. While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.¹¹⁸

The majority of the Court also rejects the Government’s argument that the imaging was constitutional because it did not “detect private activities occurring within private areas,” because in the home “all details are intimate details, [and] the entire area is held safe from prying government eyes.”¹¹⁹ The Fourth Amendment’s guarantee of sanctity to the home has never been tied to the quality of the information obtained during the investigation.¹²⁰ The majority felt holding the use of thermal imagers as unconstitutional was necessary in order to maintain a “firm line at the entrance to the house.”¹²¹

Also the limitation of use of the thermal imager to scan for only those details which are not “intimate” would be impossible for law enforcement officials to apply because an officer would not be able to know in advance whether his scan would pick up intimate details, and would be unable to determine upfront whether his scan was constitutional.¹²² Such an unpredictable definition would be counterproductive.

114. *Id.* at 2047.

115. *See id.*

116. *Id.* *See also Katz*, 389 U.S. 347.

117. *Id.*

118. *Kyllo*, 121 S. Ct. at 2044.

119. *Id.* at 2045 (emphasis in original).

120. *Id.* at 2045. There is no connection between the sophistication of the surveillance equipment and the “intimacy” of the details, noting for example that the Agema Thermovision 210 used to scan Kyllo’s home could disclose at what hour each night the lady of the house takes her daily bath, which most would consider intimate.

121. *Id.* at 2046 (quoting *Payton v. New York*, 445 U.S. 573, 590 (1980)).

122. *Id.*

tive to the officers trying to gather information for a probable cause hearing.¹²³ An “intimate” details standard would be absolutely unworkable, requiring constant litigation to determine what society considers intimate.¹²⁴ The majority also found the government’s argument that the thermal image scan did not reveal details about the home unpersuasive, because the exact purpose of using the thermal imager is to determine whether marijuana is being grown inside the home.¹²⁵

The majority of the Court agrees with the government that the Fourth Amendment never required “law enforcement officers to shield their eyes when passing by a home on public thoroughfares.”¹²⁶ This statement preserves the lawfulness of warrantless visual surveillance and upholds the plain view doctrine.¹²⁷ However, the majority feels the use of a thermal imager involves more than naked-eye surveillance.¹²⁸ In previous cases, the Court reserved judgment on how much technological enhancement of ordinary perception would still be considered visual observation.¹²⁹ In *Dow Chemical Company*, the Court upheld enhanced aerial photography of an industrial plant, but was careful to note that the area viewed was not an area “immediately adjacent to a private home, where privacy expectations are most heightened.”¹³⁰ It also found that the camera used was not a unique sensory device, which is a crucial question in the *Kyllo* analysis.¹³¹ The Court therefore rejects the notion that a thermal image scan can be analogized to the plain view doctrine, at least as long as the scanner is not in general public use.¹³²

The pivotal factor in the Court’s bright-line test is that the device used by the government must not be in general public use in order to constitute an unreasonable search without a warrant.¹³³ The dissent takes issue with this element and posits that the majority is introducing uncertainty into the Fourth Amendment analysis, rather than drawing a bright-line.¹³⁴ The dissent states, “[h]ow much use is gen-

123. See *id.*

124. See *id.*

125. *Id.* at 2043 n.2.

126. *Id.* at 2042 (quoting *California v. Ciraolo*, 476 U.S. 207, 213 (1986)).

127. *Id.*

128. *Id.* at 2043.

129. *Dow Chemical*, 476 U.S. at 237.

130. *Kyllo*, 121 S. Ct. at 2043.

131. *Id.*

132. *Id.*

133. *Id.* at 2046.

134. *Id.* at 2050.

eral public use is not even hinted at by the Court's opinion, which makes the somewhat doubtful assumption that the thermal imager used in this case does not satisfy that criterion."¹³⁵ The dissent is not only concerned about the vagueness of the rule, but is also fearful that the "threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available."¹³⁶ The majority's response to this criticism is answered in footnote six of the majority opinion, which states that the dissenters' disagreement is not with the majority, but rather with the Supreme Court's precedent.¹³⁷ The majority referred to the holding in *Ciraolo*,¹³⁸ which denominated the flights in public airways as routine, therefore preventing the defendant from having a reasonable expectation that his plants could not be observed from 1,000 feet above.¹³⁹ The Supreme Court concludes that the use of a thermal imager is not routine, and therefore declines to reexamine the factor already established by precedent.¹⁴⁰

The dissent also challenges the majority's lack of judicial restraint.¹⁴¹ The dissent contends that the issue should have properly been resolved with reference solely to the capabilities of the Agema Thermovision 210.¹⁴² However, the majority opinion states that although "the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."¹⁴³ The dissent believes such questions about future advances and capabilities would be best decided at a later date, thus giving legislators an opportunity to grapple with the emerging technology, rather than shackling them with premature constitutional guidelines.¹⁴⁴

Is *KYLLO*'S HOLDING SOUND?

The bright-line rule announced in *Kyllo* appears to be more fuzzy than bright. The dissent's attacks show the gaping holes in the majority's holding. What exactly is the definition of "general public use"? How does one go about identifying whether a device meets this defini-

135. *Id.*

136. *Id.*

137. *Id.* at 2046 n.6.

138. *California v. Ciraolo*, 476 U.S. 207 (1986).

139. *Id.*

140. *Kyllo*, 121 S. Ct. at 2046 n.6.

141. *Id.* at 2052.

142. *Id.*

143. *Id.* at 2044.

144. *Id.* at 2052.

tion? Does general public use imply that commercial availability is enough? Does it mean that one in ten people must own a thermal imager, or does it mean one out of ten thousand must own? Does general public use imply that one must be able to go to the local discount store to pick up a thermal imager? Does general public use mean one is able to obtain access to a thermal imager over the Internet? Considering that thermal imaging is not limited to law enforcement, at what point does it become so prevalent enough to be considered in general public use? These are a small sampling of possible questions behind the Court's bright-line established in *Kyllo* requiring the device to be in "general public use" in order to be classified as a reasonable search without a warrant. However, the Court gives no guidance as to how the element of "general public use" should be applied. A bright-line rule is typically intended to establish clear-cut procedure for analyzing an issue. However, this holding makes it impossible to clearly assess when the use of technology will be considered a search within the Fourth Amendment.

The application of this bright-line is not only ambiguous, but even suggests by its very language it is merely temporary. Bill Stuntz, a Harvard Law School Professor, stated, "[t]wenty years from now you may be able to buy thermal imaging technology at a Wal-Mart. . . . [t]hen either we get less privacy or the court has to draw another line."¹⁴⁵ The approach taken by the Court seems to open more questions than resolve answers. One of the overriding questions is, how long will the holding of *Kyllo* survive?

Lack of judicial restraint is another reason the Court's decision presents such problems. Judicial restraint is the philosophy of limiting decisions to the facts of each case, deciding only those issues that must be decided to resolve the case, and avoiding unnecessarily decisions on constitutional issues. The Court violated all the aspects of this philosophy. Instead of simply addressing the limited factual situation presented and the limited technology that is currently available, the Court decided to make a ruling with possible future advances in mind and unnecessarily decided constitutional issues that were not before the Court. The Court's ruling is based on the belief that one day thermal images will be capable of seeing through the walls of a home, and detecting all activities going on inside. The Court's approach in *Kyllo* is opposite of that taken by the Supreme Court in *Silverman v. United States*,¹⁴⁶ where the Court stated:

145. See Walsh, *supra* note 107, at A1.

146. *Silverman v. United States*, 365 U.S. 505 (1961).

[t]he facts of the present case, however, do not require us to consider the large questions which have been argued. We need not here contemplate the Fourth Amendment implications of these and other frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society.¹⁴⁷

The Court's abandonment of the deeply instilled philosophy of judicial restraint reeks havoc on its ruling by unnecessarily looking to possible future advances and conflicts. As a result, the holding of *Kyllo* will be short-lived before revamping or completely abandoning the decision becomes a necessity.

CONCLUSION

Perhaps American homes are more private today than they were before June 11, 2001. But the question remains: how long will this privacy last? Will the ruling established by the Supreme Court in *Kyllo* with the stated objective of protecting privacy, actually result in a reduction of American civil liberties? Only time will answer this question; yet it is unlikely that *Kyllo* will be the United States Supreme Court's last word on the issue of thermal imaging and its Fourth Amendment implications.

Sarilyn E. Hardee

147. *Id.*

PRIVACY, INTIMACY, AND ISOLATION

Julie C. Inness

Copyright © 1992 by Julie Inness

New York Oxford
OXFORD UNIVERSITY PRESS
1992

5

Information, Access, or Intimate Decisions about Our Actions? The Content of Privacy

An agent possesses privacy to the extent that she has control over certain aspects of her life. But which aspects? In other words, what is the content of privacy? Three potential lines of response to these questions emerge from the legal and philosophical literature. First of all, privacy might regulate information about ourselves¹; second of all, privacy might concern access to ourselves²; and finally, privacy might focus on intimate decisions about our actions.³ I term these responses, respectively, “information-based,” “access-based,” and “decision-based” accounts of privacy’s content.⁴ In what follows, I argue that the content of privacy cannot be captured if we focus exclusively on either information, access, or intimate decisions because privacy involves all three areas. Furthermore, I suggest that these apparently disparate areas are linked by the common denominator of intimacy—privacy’s content covers *intimate* information, access, and decisions. I conclude by offering a definition of privacy that cuts across the standard categories of information, access, or intimate decisions: privacy is the state of the agent having control over a realm of intimacy, which contains her decisions about intimate access to herself (including intimate informational access) and her decisions about her own intimate actions.

Though there are three contenders for the content of privacy, one stands apart from the others due to its extensive use in everyday, legal,

and philosophical discourse—privacy involves information about an agent.⁵ This extensive usage is readily illustrated. In everyday life, when another learns a carefully concealed fact about our sex life, behavior at home, or personal habits, we are quick to label this dissemination of information as a privacy violation.⁶ In such a case, we would explain that our privacy has been violated because it is wrong for others to distribute or obtain such personal information without our permission. Our everyday intuitions about the ties between privacy and information are mirrored in the domain of law and legislation, where privacy often assumes the role of protecting information about the individual; for example, tort privacy law is largely concerned with information protection,⁷ and state privacy legislation is chiefly designed to guard certain types of information about the agent, including information about her credit, medical, and educational history.* Finally, privacy theorists put forward such a quantity of information-based privacy definitions that understanding privacy’s content in terms of information has been termed a “dogma” of privacy theory.⁹ In perhaps the most well-known privacy definition, Alan Westin explains that privacy is “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”¹⁰ Given this proliferation of appeals to information, clearly an adequate account of privacy’s content must either explicitly include or exclude information. In what follows, I argue that some, but not all, information must be included within privacy’s scope.

Many common claims concerning information constitute representative privacy claims. This is readily illustrated. Imagine that I claim my privacy has been violated when I learn another person has informed the world in great detail about my sexual proclivities, despite my explicit request to the contrary. Two points concerning my claim are clear. First, my protest is directed against the information dissemination that has taken place; if asked why I was protesting, I might explain that others should not know detailed information about my sexual activity without my permission. Second, my identification of this information claim as a privacy claim seems to be beyond dispute. If someone were to deny this, I would not leap to the conclusion that *my* definition of privacy was in error—I would question whether *they* understood the meaning of “privacy” and suggest that *their* definition of privacy was flawed. The argument underlying this example is simple—information cannot be altogether excluded from the content of privacy.

Assuming that privacy's content is partially informational, should we allow that privacy's content is exclusively informational, that privacy is nothing more than the state of possessing control over information about ourselves? Although I accept that personal information is a component of privacy's content, I do not accept it as the identifying and constraining feature. The first problem faced by an information-based definition is that the fact that something is a piece of information about an agent is not a sufficient condition for it being within the scope of privacy. In other words, privacy does not involve control over *all* information about ourselves.¹¹ To illustrate this, consider a variety of successful attempts to gain information about me. Imagine that a stranger wishes to find out information about my sexual proclivities. She learns the desired information from my excessively talkative friend? Imagine that the stranger wishes to learn where I park my car. She learns this information from the same revealing friend.¹³ Each of these cases involves an obvious loss of control over information; however, they are not both obvious cases of lost privacy. The first case seems to involve a loss of privacy; in fact, assuming that my friend culpably distributed information, she has violated my privacy. The second case seems not to involve a privacy loss. To support these intuitions, consider what would happen if I accused my friend of lessening my privacy in the first case: the burden of proof would be on my friend to explain why a privacy loss had not occurred. If she rejected this burden, I would simply point to the nature of the information she revealed, "Look at what you revealed! It's intimate!" Without extenuating circumstances, the intimacy of sexual information places it squarely within the parameters of privacy. Yet, if I made the same accusation in the second case, the burden of proof would remain with me—*despite* the fact that there has clearly been a loss of information about myself. I would still have to justify my inclusion of **car-parking** information within the scope of privacy. The impersonal, nonintimate nature of information about a parking place usually places it outside of privacy's reach.¹⁴ As these examples reveal, neither the presence nor the absence of a privacy loss can be explained by citing the presence or absence of information distribution. We must look at the *type* of information disseminated; it is the intimacy of this information that identifies a loss of privacy.¹⁵

My argument is open to the criticism that I have drawn privacy's content closer to our linguistic intuitions only to abandon our moral intuitions: defining privacy in terms of intimate information, rather than

information as a whole, fails to account for certain of our moral intuitions. The argument supporting this criticism consists of two steps. The first step points out that including intimate information within the content of privacy allows us to morally **condemn** another when she culpably damages our control over intimate **information**—she has violated our privacy. However, excluding nonintimate information from the content of privacy has the opposite effect: we cannot condemn another for culpably lessening our control over nonintimate information since the damage does not truly constitute a privacy loss due to the nature of the information involved. The second step is prescriptive: since it is factually true that damaging someone's control over nonintimate information about herself is often morally reprehensible, it is incorrect to limit privacy's protection to intimate information. It renders us unable to condemn morally reprehensible instances of lessening another's control over nonintimate information. In order to analyze this argument, two questions must be addressed. Does an agent ever possess a moral claim to control nonintimate information about herself? If so, is this protection best described in terms of privacy?

The answer to the first question is not open to significant debate. The moral culpability of lessening or destroying an individual's control over nonintimate information in certain circumstances is readily illustrated. Imagine that a talkative friend of mine asks me what I am doing tomorrow. I reply that I am giving a surprise party for a mutual friend. My talkative friend conveys this information to others, ruining the surprise. Similarly, imagine that I tell a friend that I have taken a new job. I warn her not to repeat this information, as I wish to tell people myself. Despite this warning, she does inform others, frustrating my desire to provide the news. Do each of these examples involve morally blameworthy damage to the agent's control over nonintimate information? Yes. First of all, each of these cases involves an obvious information loss. Second of all, the information lost in both cases is not intimate. According to our society's norms, general information about a person's party plans and employment is not sufficiently personal to merit the heading of "intimate."¹⁶ If a casual acquaintance asked me about the date of a non-surprise party I was giving or the nature of my job, I might deny her this information for reasons of my own, but an exclamation of, "That's not something you should ask me about!" would be a puzzling and incomplete explanation of the reasons for my denial.¹⁷ Finally, assuming a lack of mitigating factors, both of these examples involve morally **blameworthy**

thy action on the part of the information spreader. The **information-damaged** individual can justifiably make a moral claim against the **damager**, on the grounds that the party or job information *ought* not to have been distributed without prior permission. These two examples demonstrate that my critic is at least partially correct. There are cases in which damaging someone's control over nonintimate information is morally culpable; hence, the agent does possess a moral claim to control nonintimate information about herself in certain circumstances. But is privacy a suitable foundation for this claim?

Given the chaos that surrounds privacy, it is not surprising that privacy appeals are often used to ground claims to control nonintimate information. For example, many laws and government regulations prohibiting the unauthorized distribution of nonintimate information about citizens are couched in terms of privacy.¹⁸ However, I believe this common usage confuses privacy with secrecy. An appeal to secrecy serves as an appropriate descriptive and normative foundation for our claims to control nonintimate information about ourselves and our moral condemnation of those who damage this control. To illustrate this, reconsider my previous example of the talkative friend and the surprise party information. When I tell my friend about the planned party and add, "It's a secret," my added comment conveys two meanings to my friend—the descriptive implication that the party plans are concealed information and the normative implication that she ought not inform others about my plans. If my friend proceeds to tell others, spoiling my party plans, I can explain her moral culpability by pointing to the fact that she has unjustifiably destroyed my secrecy. As this example shows, secrecy can be used to accurately describe our regulation of nonintimate information and to capture the prescriptive significance of such regulation.

A question remains unanswered: why should we prefer "secrecy" to "privacy"? After all, privacy can be used as I described above.¹⁹ Secrecy has several advantages over privacy when it comes to accurately describing control over nonintimate information. First, secrecy does not possess underlying suggestions of intimacy, as is the case with privacy. Hence, using secrecy to describe our control over nonintimate information allows us to preserve the link between privacy and intimacy. Second, secrecy is not an inherently positive concept, unlike privacy: we lack a fundamental right or claim to secrecy.²⁰ This accords with the fact that regulating nonintimate information about ourselves is not always morally acceptable—we have no right to control nonintimate information simply

qua nonintimate information; to establish such a claim, we have to explain the plans that somehow justify this control. If a census taker asks me about the number of rooms in my house, I cannot usually justifiably respond, "You have no business knowing that information!" In contrast, the positive value accorded to privacy makes privacy claims valid largely independently of our plans; the foundation of such claims lies in the fact that intimate information is, indeed, *intimate* information. Third, distinguishing secrecy from privacy allows us to distinguish between what we fear from a loss of secrecy and a loss of privacy. Secrecy involves concealing information from a specific class of people, those who could potentially damage your interests if they knew the information. As Morton Levine notes, secrecy involves concealing "information which one feels would render one vulnerable to some kind of damage. . . . If the limits of your assets were known to a potential landlord, he might not grant you a lease."²¹ The same type of concealment is also what is at stake in the case of nonintimate information regulation. For example, when I appeal to my friend not to tell others about my surprise party or new job, my goal is to conceal this information from specific others—if the people from whom I wished to conceal the information somehow learned about it, I would no longer be concerned about its concealment because I would no longer fear having my plans damaged. This contrasts with privacy, since our concern in privacy cases is to control information, not simply conceal it from those who might damage us with it. Control requires regulating information with respect to others whether or not they present any threat of damaging our interests; when I seek privacy with respect to my diary, I seek to control it with respect to humanity as a whole—I fear *anyone* accessing it without my permission. Given these points, it is clear that secrecy is capable of explaining why violating another's control over nonintimate information is morally questionable; it also provides a more satisfactory account than that provided by privacy. Hence, the conclusion is clear: privacy need not include nonintimate information within its scope if we are to explain morally reprehensible curtailments of nonintimate information control.²²

At this point, I have modified the sufficient condition for something to be within the scope of privacy—it must not be merely information about an agent, but intimate information. However, even with this modification, **information-based** accounts of privacy's content still face a problem—an information loss, even a loss of intimate information, does not constitute a necessary condition for a privacy loss. It can be lost

without another actually gaining information. There are two ways in which this can occur. First of all, a privacy loss can occur when the loss of information is only threatened. My previous example of a peeping Tom failing to see a person concealed under a bed illustrates how this might happen. In this case, the peeping Tom might be construed as having gained some form of access to the concealed individual, but clearly this has not taken the form of information acquisition. Yet the privacy loss nevertheless exists.²³ Second of all, privacy can be lost when access is breached without a gain of information. For example, when a peeping Tom looks in a person's window for the *second* time, it is conceivable that he might acquire absolutely no new information about the victim. Despite this failure, the peeping Tom clearly violates the victim's privacy with the second, as well as the first, inspection. When he is charged with, the second violation, he cannot escape with the explanation, "I've seen it all before!"

An intimate **information-based** definition of privacy will necessarily be incomplete because the loss of privacy need not involve the loss of information; yet the tie between intimate information and privacy cannot be escaped. Faced with this need to preserve the link between intimate information and privacy, while denying that intimate information is the sole constituent of privacy, let us consider the privacy accounts that claim to accomplish this: **access-based** definitions.

Access-based privacy definitions come in a multitude of forms. For example, Thomas Scanlon suggests that privacy provides us with a zone within which we need not be on the alert against intrusions and observations.²⁴ James Rachels and Jeffrey Reiman contend that privacy provides us with control over who has access, including informational access, to us.²⁵ Despite such variations, **access-based** definitions share an assumption about the content of privacy: it covers access to the agent.²⁶ Hence, the generic model of a **control-based, access-focused** privacy definition amounts to the following: privacy is the state of an agent possessing control over access to herself. With this model in mind, let us consider two questions. Does defining privacy's content in terms of access avoid the difficulties that beset **information-based** definitions? Does access to an individual cover all aspects of privacy's content? I believe that **access-based** privacy definitions are only partially successful at capturing privacy's content.

I concluded my criticism of **information-based** accounts of privacy with a question: how can we include intimate information within the

scope of privacy, while acknowledging that the dissemination of information is not necessary for the loss of privacy? Explaining privacy's content in terms of access to an individual enables us to explain how it can be lost both with *and* without the actual loss of information. On the one hand, if we accept that privacy is concerned with the regulation of access to an agent, then information loss is not necessary for the loss of privacy because an agent can damage another's access control without learning information about her; for example, a peeping Tom who looks at a victim for the tenth time is clearly damaging the victim's control over access to herself, even if no new information is revealed. On the other hand, a loss of control over intimate information can still be a privacy loss because an agent can access another by learning information about her. In other words, learning information about another can be understood as informational access, a subset of **access**.²⁷ To illustrate how a revelation of information might be an access violation, imagine that an individual manages to obtain another's love letters, which she reads without the owner's permission. This act of information acquisition is an access **violation**—the letter reader unjustifiably gains access to another through learning the information contained in the letters. In short, **access-based** definitions explain why the loss of control over information is a possible, but not necessary, route to a privacy loss—information is only one way to gain access to another.

However, **access-based** definitions of privacy are not without problems. The first one is familiar: access is not always a sufficient condition for a privacy loss. Not all forms of access diminish privacy. On the one hand, intimate access to another clearly lessens her privacy, for example, staring persistently at her, grabbing her breast, listening intently to her discussion with a friend, or learning about her sexual habits. On the other hand, nonintimate forms of access do not involve the loss of privacy. Consider the countless ways in which others access us in the course of an ordinary day: glancing at us, brushing against us in passing, hearing fragments of our conversations, learning pieces of information about our dress, hair color, and posture. Such casual, nonintimate forms of access differ in kind, rather than only in degree, from **privacy-lessening** forms of intimate access. To illustrate this, consider what would be a reasonable response to a person who protested her privacy was lessened by such forms of nonintimate access. We would point to the **type** of access involved, stressing the point that this **type** of access does not constitute a decrease of privacy. If she rejected this explanation, the burden of proof

would be on *her* to convince us that these apparently nonintimate, nonprivate forms of access were, in reality, sufficiently intimate to merit privacy. If privacy claims concerning access have to be couched in terms of intimacy, then we must reject unmodified access definitions of privacy.²⁸

We have found a sufficient condition for a loss of privacy in the form of violating another's control over intimate access to herself. However, although many privacy issues revolve around access regulation, that does not exhaust the field of privacy. Intimate decisions also appear to fall within the scope of privacy, as is evident in both law and our everyday intuitions; for example, questions of access are peripheral to the majority of constitutional privacy cases. Constitutional law focuses on “a privacy interest with reference to certain *decisions* that are properly for the individual to make.”²⁹ The decisions that the Supreme Court has protected under the rubric of privacy include those about such intimate activities as child rearing and education, family relationships, procreation, marriage, contraception, and abortion.³⁰ The Court’s rationale for including an agent’s decisions about such activities within the content of privacy explicitly appeals to their *intimacy*; according to the Court, it is *because* such decisions are intimate that they belong within the sphere of an agent’s constitutional right to privacy. This inclusion is not peculiar to the Supreme Court. We commonly distinguish between intimate and nonintimate decisions about our actions, characterizing intimate decisions as “private” or “personal”—unfit subjects for the state’s regulatory power. Consider the difference between being informed that the social welfare mandates that we must engage in sexual activity with specified individuals and being informed that the social welfare mandates that we must pay taxes. Our liberty of action is curtailed in each case, yet these curtailments are not identical. Decisions concerning sexual activity and sexual partners are not the type of decisions that can be dictated by the social welfare, barring extraordinary social hardship, while the social welfare seems a reasonable justification for taxes. If asked to justify these different conclusions, we might respond that the decision to engage in sex with a particular individual is a private matter—our privacy is damaged if the decision is forced—while decisions about taxes are neither intimate nor private. This response constitutes an understandable defense. It accords with our underlying intuition that intimate decisions about our actions belong with the realm of privacy, while nonintimate decisions about our actions fall outside of this realm. Given this legal and everyday

intuition that constitutional privacy issues are part of privacy’s content, must we discard our definition of privacy in terms of the agent’s control over intimate access?³¹ Not necessarily.

Faced with the apparent conflict between decisional and access accounts of privacy, some have argued that “decisional privacy” is a misnomer: it is actually nothing more than liberty or freedom attached to a misleading description. As Ruth Gavison explains, “identifying privacy as noninterference with private action . . . may obscure the nature of the legal decision and draw attention away from important considerations. The limit of state interference with individual action is an important question that has been with us for centuries. The usual terminology for dealing with this question is that of ‘liberty of action.’”³² According to this view, claiming that intimate decisions are protected by privacy is identical to claiming intimate decisions are protected by “liberty of action.” Furthermore, the rubric “liberty of action” has the advantage of historical precedent. Assuming, as does Gavison, that matters of regulating access are at the conceptual core of privacy, matters that are conceptually distinct from liberty of action (since they involve duties of noninterference on the part of others), we merely muddy the theoretical waters by speaking of privacy with respect to intimate decisions. Thus, although we should retain intimate access for privacy’s content, we should exclude decisional matters as best belonging within the sphere of liberty of action.

The argument that we should abandon constitutional privacy on the grounds that it is nothing more than liberty of action is initially plausible. After all, even cursory consideration shows that the intimate decisions protected by constitutional privacy delineate a realm of liberty of action. For example, if I have a privacy right to control my childbearing, I can also be said to possess liberty of action with respect to childbearing. Similarly, if I have a privacy right to control my sexual expression in most situations, I can also be said to possess liberty of action with respect to my sexuality. Despite its initial plausibility, the argument that attempts to dissolve decisional privacy into liberty of action suffers from three flaws. First, it does not provide a defense against the argument that decisional/constitutional privacy involves liberties that possess a feature distinguishing them from nonprivacy liberties. Second, it offers no explanation of how we have come to confuse privacy and liberty of action. Third, if we accept this argument, it also undermines access-based privacy theories, pulling the rug out from under itself. Let me

expand upon these points. According to the first criticism, the link between constitutional privacy and liberty of action can be interpreted in two ways—as indicating that decisional privacy is a confused concept or as pointing to something distinctive about privacy-protected liberty of action. Given that we *do* distinguish between privacy-invoking liberty of action and liberty of action not protected by privacy, surely it is more plausible to seek the basis for this distinction than to abandon it as confused. Turning to the second criticism, we possess no particular reason to believe that we have indeed confused liberty of action with decisional privacy—Ruth Gavison’s argument lacks any explanation of the birth of our “confusion.” Finally, if we were to accept her argument (in the spirit of **Ockham**), our razor would cut too far for the access theorist. Although constitutional privacy most clearly covers certain liberties, the same can be said of access-based definitions of privacy; for example, if I have a privacy claim to control access to myself, thus limiting a peeping Tom’s access, I can also be said to have a certain liberty, namely, the liberty to exercise this control. Thus, if we reject decisional privacy because of its tie to liberty, we also have grounds to reject access-control definitions of privacy. Given the centrality of access regulation to privacy, we have every reason to reject an argument that leads to its abandonment. Faced with these criticisms, a privacy theorist cannot abandon decisional privacy by merely linking it to liberty of action.

Once again, we are faced with a quandary. Changing privacy’s content from intimate information to intimate access has its advantages. By so doing, we retain intimate information (in the guise of informational access) within the scope of privacy, while broadening privacy’s scope to include noninformational intimate access. Nevertheless, this change does not help us when we are faced with privacy that involves protecting an agent’s intimate decisions about her own actions; these decisions cannot be compressed into access matters. Yet the tie between an individual’s intimate decisions about her actions and privacy has resisted criticism. Therefore, explaining privacy’s content in terms of access does not encompass its entire content. How are we to resolve the apparently conflicting demands of decisional and access privacy?

An agent’s intimate decisions about her own actions seem to be inescapably within the domain of privacy. Yet matters of intimate access also seem to be within this domain. There are two ways in which the conflict between these apparently disparate aspects of privacy can be

resolved. First of all, intimate access can be rejected as part of privacy; privacy involves *only* control over intimate decisions about an individual’s own actions. Second of all, both intimate access and intimate decisions can be included within privacy’s content by offering an explanation of what ties together these disparate areas. In what follows, I argue that explaining privacy’s content only in terms of an agent’s intimate decisions about her actions is unsatisfactory since matters of intimate access and informational access also fall within privacy’s domain, but including intimate access and an agent’s intimate decisions about her actions within privacy’s content is satisfactory. The factor tying together these seemingly disparate areas of privacy is their intimacy.

Given the apparent dissimilarity between an agent’s intimate decisions about her actions and questions of intimate access, it is tempting to “explain” this dissimilarity by simply excluding intimate access from the content of privacy. This is not an uncommon path to follow; constitutional privacy cases never explain how decisional privacy relates to tort law (access) privacy, leaving the impression that decisional privacy is “true” privacy. This impression is strengthened when we turn to the work of several theorists who have commented on constitutional privacy. These privacy theorists attempt to provide a coherent theoretical framework for constitutional privacy, but they neglect to provide a framework large enough to include matters of intimate access.³³ However, can access matters simply be removed from the scope of privacy, given their prevalence within the field of privacy? Certainly not without an argument; but the only plausible one has previously proven to be unsuccessful. We could reverse the “liberty argument” provided by access theorists against decisional privacy (in other words, control over intimate access could be described as a matter of liberty, and hence, not a privacy issue), but this reversal would fall victim to the criticisms I directed at it in its original form. Barring this move, intimate access issues cannot be removed from the content of privacy, due to their prevalence in ordinary linguistic usage and tort law, and our lack of any reason to think that this prevalence is based on confusion.

There remains one final route: we must incorporate both intimate access to an agent and an agent’s intimate decisions about her own actions into the content of privacy. The obstacle standing in the way of this incorporation is the apparent lack of a conceptual tie between decisional and access privacy issues. Ruth Gavison believes that the lack of such an apparent tie entails a rejection of decisional privacy:

If the concepts we use give the appearance of differentiating concerns without in fact isolating something distinct, we are likely to fall victims to this false appearance and our chosen language will be a hindrance rather than a help. The reason for excluding [decisional privacy situations] is that they present precisely such a **danger**.³⁴

Although Gavison's argument is designed to exclude decisional privacy, it can be reversed to exclude matters of access from privacy's content (assuming we reject Gavison's intuition that access matters are more basic to privacy than decisional matters). Either way, the crux of it remains the same—assimilating decisions about actions and access matters under the common heading of "privacy" represents a loss of conceptual focus.

Fortunately, after considering the nature of the decisions and matters of access that have been brought within the scope of privacy in this book, the force of this criticism is lost. I have **not** argued that all forms of access or decisions about actions are included in privacy's content. I have argued that *intimate* access and decisions about actions fall within privacy's domain. Hence, there is a conceptual focus uniting the decisional and access aspects of **privacy—the** shared focus on intimacy. Rather than seeing privacy as composed of two disparate elements, we should understand it as protecting a realm of intimacy, a realm that happens to have both access and liberty of action aspects. Given that intimacy is the "something distinct" about decisional and access privacy, Gavison's argument collapses.

Having argued that both an agent's intimate decisions about her own actions and intimate access to the agent (including intimate informational access) belong within privacy's content, I now wish to perform a curious backtrack. As I have previously indicated, many privacy theorists assume that there is an important structural distinction between decision and **access-based** privacy.³⁵ It is simple to see what underlies this assumption. On the one hand, privacy restrictions on intimate access (including intimate informational access) are primarily designed to give rise to duties of noninterference on the part of **others**. For example, when I seek privacy with respect to access to areas of my body, I seek to impose duties on others not to access my body without permission. On the other hand, the intimate decisional privacy issues protected by constitutional privacy law concern the **agent's** own intimate actions. For example, when I seek privacy with respect to my decisions about contraception, I am primarily concerned with possessing freedom of action with regard to

my use of contraceptives. However, this division is not as distinct as it initially appears. Consider a privacy claim concerning a matter of intimate access, for example, with respect to being touched by others or with respect to having a diary read by others. In making such a claim, we do not seek to avoid all access by others; we seek control over **decisions** about intimate access to ourselves. We wish to be free to decide who may access us. Consider also a privacy claim concerning a matter of "decisional privacy," for example, concerning a decision about abortion or a decision about sexual activity with a consenting partner. Such claims are claims to have control over **decisions** concerning our intimate actions. We wish to be free to decide how to act with respect to intimate situations. In short, both "access" and "decisional" privacy claims are claims to have control over **decisions**; hence, the distinction between decision-based and access-based privacy collapses. Rather than understanding privacy's content in terms of intimate access **and** intimate decisions, we should draw together these seemingly disparate areas: privacy's content covers intimate decisions, including the agent's decisions concerning intimate access to herself (including informational access) and her decisions about her own intimate actions.³⁶ In the following chapters, my discussion of intimate decisions will cover both types of decision.

It may appear that I have provided all the pieces necessary for an adequate definition of privacy. Starting with the initial assumption that privacy provides the individual with control over certain aspects of her life, I have shown that the content of privacy includes our decisions about intimate informational access, intimate access, and our own intimate actions. The intimacy of these aspects of privacy constitutes the conceptual focus of privacy. Putting together these pieces, privacy can be defined as the state of an agent possessing control over a realm of intimacy, which includes her decisions about intimate informational access, intimate access, and intimate actions. Yet there remains a deficiency in this privacy definition: it depends upon the notion of intimacy, yet I have not defined intimacy. The next chapter supplies this definition.

Notes

1. Assuming that privacy works through control, an **information-based** definition of privacy would be "privacy is the state of possessing control over information about yourself." For examples of **information-based** definitions of

privacy, see Judith Jarvis Thomson, "The Right to Privacy," *Philosophy and Public Affairs* 4 (1975): 295–314; Charles Fried, "Privacy," *Yale Law Journal* 77 (1968): 475–93; Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967); Elizabeth Beardsley, "Privacy: Autonomy and Selective Disclosure," in *Privacy: Nomos XIII*, ed. J. Roland Pennock and John W. Chapman (New York: Atherton Press, 1971), 56–70; Richard Wasserstrom, "Privacy: Some Arguments and Assumptions," in *Philosophical Law*, ed. Richard Bronaugh (Westport, CT: Greenwood Press, 1978), 148–66.

2. Assuming that privacy functions through control, an access-based definition of privacy amounts to "privacy is the state of possessing control over access to your self." For examples of access-based privacy definitions, see Jeffrey Reiman, "Privacy, Intimacy and Personhood," *Philosophy and Public Affairs* 6 (1976): 26–44; James Rachels, "Why Privacy Is Important," *Philosophy and Public Affairs* 4 (1975): 323–33; Richard Parker, "A Definition of Privacy," *Rutgers Law Review* 27 (1974): 275–96; Thomas Scanlon, "Thomson on Privacy," *Philosophy and Public Affairs* 4 (1975): 315–22.

3. Assuming that privacy functions through control, a definition of privacy based on intimate decisions amounts to "privacy is the state of possessing control over the making and implementation of intimate decisions about your actions." For examples of intimate decision based privacy definitions, see Tom Gerety, "Redefining Privacy," *Harvard Civil Rights–Civil Liberties Law Review* 12 (1977): 233–96; June Eichbaum, "Towards an Autonomy-Based Theory of Constitutional Privacy: Beyond the Ideology of Familial Privacy," *Harvard Civil Rights–Civil Liberties Law Review* 14 (1979): 361–84; David A. J. Richards, "Unnatural Acts and the Constitutional Right to Privacy," *Fordham Law Review* 45 (1977): 1312–48.

4. Note that these labels are used only to accord with common usage in the privacy literature. Clearly, giving the agent control over information or access to herself can be described as giving her control over certain decisions. For the purposes of this chapter, decisional privacy is equivalent to constitutional privacy.

5. Information about the agent should not be narrowly construed; it can be information about her behavior, plans, or other aspects of her life.

6. The objection might be raised that I am describing a situation where privacy has been merely *lost*, not *violated*. Only if the person has gathered the information in a culpable manner should we take the additional step of describing the privacy loss as a privacy violation. I accept that a loss of privacy may not be a morally culpable violation; an agent might justifiably or simply inadvertently lessen the privacy of another. However, I believe that the term "violation" should be retained for both culpable and nonculpable cases of lessened privacy. This term makes it clear that we have a *prima facie* claim to privacy since privacy is a presumptive good; when someone lessens another's privacy, they violate her in a

way that demands explanation. If they offer a satisfactory explanation, they may avoid blame for their violation, yet the violation still remains real: by losing privacy, the agent has lost something of value to herself; she has been damaged, even if no one is held culpable for the damage.

7. This is understandable, given that tort privacy law is claimed to have developed due to a lawyer's desire to create a legal redress against the yellow journalism of his time. See Samuel Warren and Louis Brandeis, "The Right to Privacy," *The Harvard Law Review* 4 (1890): 193–220.

8. To illustrate this, consider California's Right to Privacy Law.

9. William A. Parent, "Recent Work on the Concept of Privacy," *American Philosophical Quarterly* 4 (1983): 343.

10. Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967), 7.

11. This fact overturns a number of information-based privacy definitions, such as Alan Westin's.

12. Though I focus this example on the revelation of sexual information, my argument covers other types of intimate information, such as information about my family life, love affairs, or inner thoughts:

13. Although I focus on information concerning a parking place, any number of informational alternatives could be substituted involving other instances of impersonal information dissemination, for example, my talkative friend could reveal my car's color, the nature of my job, or the timber of my voice.

14. This is not to suggest that information about a parking place is *necessarily* outside of the scope of privacy. It is to suggest that the burden of proof is on the agent to explain why information about her parking place is intimate.

15. Of course, we *could* contend that all information is private, including information about a parking place. I am willing to accept this modification, but it does nothing more than reword the privacy theorist's task—she still has to determine why certain types of information are "essentially private."

I do not mean to suggest that the boundary between intimate and nonintimate information is clear; it is not. For example, a nonintimate piece of information may become intimate strictly on the basis of where it is located: if I write about the weather in my personal journal, I can still justifiably claim that my privacy was invaded if another reads my weather report without permission.

16. This is not to suggest that all information about parties and employment is necessarily nonintimate; it is only to suggest that the vague information involved in my examples does not have the status of intimate information.

17. Compare this to my reaction upon being questioned about truly private information. If I were questioned by a stranger about my sex life, an exclamation of, "That's not something you should ask me about!" would constitute a satisfactory rejoinder.

18. For an example of this, see the Federal Privacy Act.

19. I could describe what took place in both the party and job information

example as a “privacy violation” without committing an obvious verbal error. Furthermore, my description would probably successfully convey my intended meaning, including its prescriptive aspect, i.e., the teller of the information told something she ought not to have told.

20. Though we canjustify secrecy claims in many circumstances. We have an expansive **property-based** secrecy claim with respect to much nonintimate information; for example, clearly I have a justified secrecy claim to control my own information about the profitable computer technology I have been fortunate enough to develop, since it is **my** property. The Constitution’s protection against nonintimate search and seizure partially acknowledges the importance of protecting secrecy claims with respect to property.

21. Morton Levine, “Privacy in the Tradition of the Western World,” in *Privacy*, ed. William Bier (New York: Fordham University Press, 1980), 19.

22. Since this work focuses on privacy, I will not discuss secrecy at greater length. For further information about the relation between privacy and secrecy, see Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (New York: Random House, 1983).

23. Assume that the victim hid sufficiently rapidly that the peeping Tom did not even learn where she had hidden, since this knowledge might be construed as an acquisition of information about the agent.

24. Scanlon, “Thomson on Privacy,” 320.

25. See Rachels, “Why Privacy Is Important,” 329; and Reiman, “Privacy, Intimacy and Personhood.”

26. “Access to an individual” should be broadly construed. It should not be understood as involving only direct contact through the senses with the individual. We can also gain access through intermediary sources or even by merely entering into her “personal space.” For example, reading someone’s private journal without her permission would count as gaining access to the individual, as would learning a piece of information about her, which reveals the continuity between the information and access-based privacy accounts.

27. Note that this interpretation of access as including a subset of informational access will be accepted in the remainder of this work.

28. An access privacy theorist might respond that our intuitions are confused: someone glancing at a woman’s hands *does* lessen her privacy in the same way as someone grabbing her breast since both actions involve uncontrolled access. Yet we still have to explain why certain access violations, such as breast grabbing, are so much more significant than others. The obvious answer would be that certain areas of the body, such as a woman’s breasts, are “private,” while others are not, but this does no more than restate the problem. The access theorist still has to explain why certain forms of access, intimate ones, are at the core of privacy.

29. See *Bowers v. Hardwick*, minority opinion, 85 U.S. 140 (1986).

30. See *Bowers v. Hardwick*, majority opinion.

31. Note that I use “constitutional privacy issues” as a synonym for decisional privacy with respect to our actions.

32. Ruth Gavison, “Privacy and the Limits of Law,” in *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand Schoeman (New York: Cambridge University Press, 1984), 358.

33. For examples, see Eichbaum, “Towards an Autonomy-Based Theory of Constitutional Privacy”; and David A. J. Richards, *Toleration and the Constitution* (New York: Oxford University Press, 1986).

34. Gavison, “Privacy and the Limits of Law,” 357.

35. For example, see Gavison, “Privacy and the Limits of Law.”

36. The reason why I avoided grouping together “decisional” and “access” privacy is that this move would have abandoned the divisions commonly found in privacy theory and failed to simplify the task at hand. The problem of linking together an agent’s decisions about informational access, noninformational access, and intimate actions would have remained in need of a solution.



AMERICAN CONSTITUTIONAL LAW

Otis H. Stephens, Jr.
John M. Scheb, II

Department of Political Science
University of Tennessee, Knoxville

Copyright © 1993 BY WEST PUBLISHING COMPANY

W E S T P U B L I S H I N G C O M P A N Y

Minneapolis/St. Paul • New York • Los Angeles • San Francisco

Katz v. United States

389 U.S..347; 88 S. Ct. 507; 19 L. Ed. 2d 576(1967)

Vote: 7-1

Mr. Justice Stewart delivered the opinion of the court.

The petitioner was convicted in the District Court for the Southern District of California under an eight-count indictment charging him with transmitting wagering information by telephone from Los Angeles to Miami and Boston in violation of a federal statute. At trial the Government was permitted, over the petitioner's objection, to introduce evidence of the petitioner's end of telephone conversations, overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls. In affirming his conviction, the Court of Appeals rejected the contention that the recordings had been obtained in violation of the Fourth Amendment, because "[t]here was no physical entrance into the area occupied by [the petitioner]."¹ We granted *certiorari* in order to consider the constitutional questions thus presented.

The petitioner has phrased those questions as follows:

A. Whether a public telephone booth is a constitutionally protected area so that evidence obtained by attaching an electronic listening recording device to the top of such a booth is obtained in violation of the right to privacy of the user of the booth.

B. Whether physical penetration of a constitutionally protected area is necessary before a search and seizure can be said to be violative of the Fourth Amendment to the United States Constitution.

We decline to adopt this formulation of the issues. In the first place the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase "constitutionally protected area." Secondly, the Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion. But the protection of a person's general right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States.

Because of the misleading way the issues have been formulated, the parties have attached great significance to the characterization of the telephone booth from which the petitioner placed his calls. The petitioner has strenuously argued that the booth was a "constitutionally protected area." The Government has maintained with equal vigor that it was not. But

this effort to decide whether or not a given “area,” viewed in the abstract, is “constitutionallyprotected” deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

The Government stresses the fact that the telephone booth from which the petitioner made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside. But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend’s apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

The Government contends, however, that the activities of its agents in this case should not be tested by Fourth Amendment requirements, for the surveillance technique they employed involved no physical penetration of the telephone booth from which the petitioner placed his calls. It is true that the absence of such penetration was at one time thought to foreclose further Fourth Amendment inquiry, *** for that Amendment was thought to limit only searches and seizures of tangible property. But “[t]he premise that property interests control the right of the Government to search and seize has been discredited.” Thus, although a closely divided Court supposed in *Olmstead* that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested. Indeed, we have expressly held that the

Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements overheard without any “technical trespass under . . . local property law.” Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people—and not simply “areas”—against unreasonable searches and seizures it becomes clear that the reach of the Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.

We conclude that the underpinnings of . . . *Olmstead v. United States* . . . have been so eroded by our subsequent decisions that the “trespass” doctrine there enunciated can no longer be regarded as controlling. The Government’s activities in electronically listening to and recording the petitioner’s words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a “search and seizure” within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.

The question remaining for decision, then, is whether the search and seizure conducted in this case complied with constitutional standards. In that regard, the Government’s position is that its agents acted in an entirely defensible manner. They did not begin their electronic surveillance until investigation of the petitioner’s activities had established a strong probability that he was using the telephone in question to transmit gambling information to persons in other States, in violation of federal law. Moreover, the surveillance was limited, both in scope and in duration, to the specific purpose of establishing the contents of the petitioner’s unlawful telephone communications. The agents confined their surveillance to the brief periods during which he used the telephone booth, and they took great care to overhear only the conversations of the petitioner himself.

Accepting this account of the Government’s actions as accurate, it is clear that this surveillance was so narrowly circumscribed that a duly authorized magistrate, properly notified of the need for such investigation, specifically informed of the basis on which it was to proceed, and clearly apprised of the precise intrusion it would entail, could constitution-

ally have authorized, with appropriate safeguards, the very limited search and seizure that the Government asserts in fact took place.

The Government urges that, because its agents . . . did no more here than they might properly have done with prior judicial sanction, we should retroactively validate their conduct. That we cannot do. It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized. In the absence of such safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end. Searches conducted without warrants have been held unlawful “notwithstanding facts unquestionably showing probable cause,” for the Constitution requires “that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police. . . .” “Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes,” and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.

It is difficult to imagine how any of those exceptions could ever apply to the sort of search and seizure involved in this case. Even electronic surveillance substantially contemporaneous with an individual’s arrest could hardly be deemed an “incident” of that arrest. Nor could the use of electronic surveillance without prior authorization be justified on grounds of “hot pursuit.” And, of course, the very nature of electronic surveillance precludes its use pursuant to the suspect’s consent.

The Government does not question these basic principles. Rather, it urges the creation of a new exception to cover this case. It argues that surveillance of a telephone booth should be exempted from the usual requirement of advance authorization by a magistrate upon a showing of probable cause. We cannot agree. Omission of such authorization bypasses the safeguards provided by an objective predetermination of probable cause, and substitutes instead the far less reliable procedure of an after-the-event justification for the . . . search, too likely to be subtly influenced by the familiar shortcomings of hindsight judgment. ***

And bypassing a neutral predetermination of the scope of a search leaves individuals secure from Fourth Amendment violations “only in the discretion of the police.” ***

These considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth. Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures. The government agents here ignored “the procedure of antecedent justification . . . that is central to the Fourth Amendment,” *** a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case. Because the surveillance here failed to meet that condition, and because it led to the petitioner’s conviction, the judgment must be reversed.

Mr. Justice Marshall took no part in the consideration or decision of this case.

Mr. Justice Douglas, with whom **Mr. Justice Brennan** joins, concurring. . . .

Mr. Justice Harlan, concurring.

I join the opinion of the Court, which I read to hold only (a) that an enclosed telephone booth is an area where, like a home, a person has a constitutionally protected reasonable expectation of privacy; (b) that electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment; and (c) that the invasion of a constitutionally protected area by fed-

eral authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant.

As the Court's opinion states, "the Fourth Amendment protects people, not places." The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a "place." My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.

The critical fact in this case is that "[o]ne who occupies it [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume" that his conversation is not being intercepted. The point is not that the booth is "accessible to the public" at other times, but that it is a temporarily private place whose momentary occupants expectations of freedom from intrusion are recognized as reasonable....

Mr. Justice White, concurring....

Mr. Justice Black, dissenting.

My basic objection is twofold: (1) I do not believe that the words of the Amendment will bear the meaning given them by today's decision, and (2) I do not believe that it is the proper role of this Court to rewrite the Amendment in order "to bring it into harmony with the times" and thus reach a result that many people believe to be desirable.

While I realize that an argument based on the meaning of words lacks the scope, and no doubt the appeal, of broad policy discussions and philosophical discourses on such nebulous subjects as privacy, for me the language of the Amendment is the crucial

place to look in construing a written document such as our Constitution. The Fourth Amendment says that The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The first clause protects "persons, houses, papers, and effects, against unreasonable searches and seizures...." These words connote the idea of tangible things with size, form, and weight, things capable of being searched, seized, or both. The second clause of the Amendment still further established its Framers' purpose to limit its protection to tangible things by providing that no warrants shall issue but those "particularly describing the place to be searched, and the persons or things to be seized." A conversation overheard by eavesdropping, whether by plain snooping or wire-tapping, is not tangible and, under the normally accepted meanings of the words, can neither be searched nor seized. In addition the language of the second clause indicates that the Amendment refers not only to something tangible so it can be seized but to something already in existence so it can be described. Yet the Court's interpretation would have the Amendment apply to overhearing future conversations which by their very nature are nonexistent until they take place. How can one "describe" a future conversation, and, if one cannot, how can a magistrate issue a warrant to eavesdrop one in the future? It is argued that information showing what is expected to be said is sufficient to limit the boundaries of what later can be admitted into evidence; but does such general information really meet the specific language of the Amendment which says "particularly describing"? Rather than using language in a completely artificial way, I must conclude that the Fourth Amendment simply does not apply to eavesdropping.

Tapping telephone wires, of course, was an unknown possibility at the time the Fourth Amendment was adopted. But eavesdropping (and wiretapping) is nothing more than eavesdropping by telephone) was, "an ancient practice which at common law was condemned as a nuisance. In those days the eavesdropper listened by naked ear under the eaves of

houses or their windows, or beyond their walls seeking out private discourse."*** There can be no doubt that the Framers were aware of this practice, and if they had desired to outlaw or restrict the use of evidence obtained by eavesdropping, I believe that they would have used the appropriate language to do so in the Fourth Amendment. They certainly would not have left such a task to the ingenuity of language-stretching judges. No one, it seems to me, can read the debates on the Bill of Rights without reaching the conclusion that its Framers and critics well knew the meaning of the words they used, what they would be understood to mean by others, their scope and their limitations. Under these circumstances it strikes me as a charge against their scholarship, their common sense and their candor to give to the Fourth Amendment's language the eavesdropping meaning the Court imputes to it today.

I do not deny that common sense requires and that this Court often has said that the Bill of Rights' safeguards should be given a liberal construction. This principle, however, does not justify construing the search and seizure amendment as applying to eavesdropping or the "seizure" of conversations. The

Fourth Amendment was aimed directly at the abhorred practice of breaking in, ransacking and searching homes and other buildings and seizing people's personal belongings without warrants issued by magistrates. The Amendment deserves, and this Court has given it, a liberal construction in order to protect against warrantless searches of buildings and seizures of tangible personal effects. But until today this Court has refused to say that eavesdropping comes within the ambit of Fourth Amendment restrictions.

Since I see no way in which the words of the Fourth Amendment can be construed to apply to eavesdropping, that closes the matter for me. In interpreting the Bill of Rights, I willingly go as far as a liberal construction of the language takes me, but I simply cannot in good conscience give a meaning to words which they have never before been thought to have and which they certainly do not have in common ordinary usage. I will not distort the words of the Amendment in order to "keep the Constitution up to date" or "to bring it into harmony with the time." It was never meant that this Court have such power, which in effect would make us a continuously functioning constitutional convention.

PAVESICH, PROPERTY AND PRIVACY: THE COMMON ORIGINS OF PROPERTY RIGHTS AND PRIVACY RIGHTS IN GEORGIA

MICHAEL B. KENT, JR.*

* Assistant Professor of Law, John Marshall Law School. I would like to thank the editors and staff of the *John Marshall Law Journal*, especially Amanda Gaddis and John Duncan, for their editorial and research assistance.

II. PAVESICH v. NEW ENGLAND LIFE INSURANCE CO.

The interconnection between property and privacy is unmistakable when one considers how these rights have developed in Georgia. And Georgia law (regarding this subject, at any rate) is quite significant. In 1905, with the state Supreme Court's unanimous decision in *Pavesich v. New England Life Insurance Co.*,¹⁰ Georgia became the first jurisdiction to recognize privacy as a specific, remediable common-law right.

Pavesich arose when the defendant life insurance company published a photograph of artist Paolo Pavesich in a newspaper advertisement. The company had acquired the picture from an Atlanta photographer, who gave it to the insurance company without Pavesich's permission. In the advertisement, Pavesich was portrayed as a vigorous and responsible individual that had purchased life insurance from the company "in [the] healthy and productive period of life."¹¹ By virtue of this apparently intelligent decision, the advertisement portrayed Pavesich as resting easy, not only because his family would be protected after his demise, but also because of the annual dividends he received from the policies during his lifetime.¹² Next to the picture of Pavesich, the advertisement contained the photograph of "an ill-dressed and sickly looking person," who purportedly did not have Pavesich's foresight and now, unable to secure insurance, realized his mistake.¹³ Of course, the portrayal of Pavesich was entirely fictitious, as he had neither purchased a life insurance policy from the company nor made the statements attributed to him. Thus, Pavesich complained that the advertisement was "peculiarly offensive to him" and had a tendency to "ridicule him before the world, and especially with his friends and acquaintances" who knew the substance of the advertisement to be false.¹⁴

label attached to other rights – most notably those of property and contract – and, therefore, "is superfluous" as a separate legal doctrine. See Amy Peikoff, *No Corn on this Cobb: Why Reductionists Should be All Ears for Pavesich*, 42 BRANDEIS L. J. 751, 751-52 (2004).

10. 50 S.E. 68 (Ga. 1905).

11. *Id.* at 69.

12. *Id.*

13. *Id.* at 68-69.

14. *Id.* at 69.

As a result, Pavesich filed suit against the company, its general agent, and the photographer. Although Pavesich accused the defendants of acting maliciously in a manner that adversely affected his reputation, he did not assert an explicit action for defamation. Rather, Pavesich claimed that the advertisement constituted a “trespass upon [his] right of privacy.”¹⁵ The trial court rejected this claim, a result that, given the state of the legal landscape at the time, could not have been too surprising for Pavesich’s lawyer. Although some courts previously had hinted that a right to privacy might exist, none had explicitly recognized such a right as an independent ground for legal action.

Indeed, the most prominent argument for an independent privacy right came not from the case law, but rather from an article by Samuel Warren and Louis Brandeis published more than a decade earlier in the *Harvard Law Review*.¹⁶ In their article, Warren and Brandeis had argued that “a general right to privacy”¹⁷ could be gleaned from existing cases – most notably, the common law’s treatment of manuscripts, works of art, and other types of intellectual property.¹⁸ At the time *Pavesich* was decided, however, no court of last resort had yet agreed.

In fact, the most famous court to have addressed the issue refused to recognize an independent right of privacy on very similar facts. In *Roberson v. Rochester Folding Box Co.*,¹⁹ the New York Court of Appeals rejected a privacy claim brought by a woman whose picture had been used, without her consent, on flyers advertising the defendant’s flour.²⁰ Even though the lower court had sustained her cause of action based on “the right to be let alone,” the Court of Appeals balked due to the lack of legal precedent supporting such a right:

Mention of such a right is not to be found in Blackstone, Kent, or any other of the great commentators upon the law; nor, so far as the learning of counsel or the courts in this case have been able to discover, does its existence seem to have been asserted prior to about the year 1890, when it was

15. *Id.*

16. See generally Warren & Brandeis, *supra* note 2, at 193-220.

17. *Id.* at 198.

18. *Id.* at 205.

19. 64 N.E. 442 (N.Y. 1902).

20. *Id.* at 442.

presented with attractiveness, and no inconsiderable ability,
in the Harvard Law Review . . .²¹

Thus, the New York court insisted that the only authority for recognizing a right to privacy was that offered by Warren and Brandeis, and the precedents relied on by those authors admittedly did not recognize a right to privacy as such. Rather (as the Georgia Supreme Court would point out), all of the cases on which Warren and Brandeis could have relied were “based either upon the recognition of a right of property, or upon the fact that the publication would be a breach of contract, confidence, or trust.”²² By the time Paolo Pavesich’s case reached the Georgia high court, it faced a decidedly uphill battle. The question confronting the court – a question which no other court of last resort had answered affirmatively – was “whether an individual has a right of privacy which he can enforce, and which the court will protect against invasion.”²³ Answering that question in the affirmative, Justice Andrew J. Cobb, writing for a unanimous court, made history.

Unfortunately, *Pavesich* has not always received the attention it deserves. Many commentators have glossed over the decision as a mere endorsement of the arguments made by Warren and Brandeis,²⁴ arguments that some commentators have criticized as unpersuasive and unsupported.²⁵ But *Pavesich* did more. As one scholar recently has posited, *Pavesich* “contributed something crucial”²⁶ to the debate over privacy – a justification grounded not only in appeals to prior precedent or pragmatic policy concerns, but in political and moral philosophy as well.²⁷ Included in the *Pavesich* opinion are allusions to natural law and social compact theory, references to Blackstone and his

21. *Id.* at 443.

22. *Pavesich*, 50 S.E. at 75.

23. *Id.* at 69.

24. See, e.g., William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 386 (1960) (suggesting that *Pavesich* “accepted the views of Warren and Brandeis”); see also Haeji Hong, *Dismantling the Private Enforcement of the Privacy Act of 1974: Doe v. Chao*, 38 AKRON L. REV. 71, 75 (2005) (stating that *Pavesich* “embraced the right to privacy set forth by Warren and Brandeis”).

25. See, e.g., Peikoff, *supra* note 9, at 773.

26. *Id.* at 755.

27. *Id.* at 783-91 (analyzing *Pavesich* decision).

conception of absolute or fundamental rights, and the use of precedent and language littered with deep-rooted, property-based associations. These various elements of the opinion supported legal recognition of a right to privacy in a manner that was different from (and, in my opinion, more persuasive than) what had come before.²⁸ More importantly for present purposes, a careful evaluation of these different elements, in light of both prior and subsequent authority, demonstrates the close relationship between the rights of privacy and property.

A. Natural Law and the Social Compact

Because no precedent affirmatively supported an independent right of privacy, Justice Cobb and his colleagues on the Georgia court had to look elsewhere for the foundations of their argument. Importantly for our purposes, the first place they turned was to the branch of political philosophy characterized by social compact theory. “The individual,” explained Justice Cobb, “surrenders to society many rights and privileges which he would be free to exercise in a state of nature, in exchange for the benefits which he receives as a member of society.”²⁹ Thus, at the outset, Justice Cobb grounded his analysis in the idea that individuals enjoy certain rights under natural law, regardless of any action or inaction by the state. Individuals agree to yield some of these natural rights in order to promote the soundness of the commonwealth (i.e., “as a member of society”), in exchange for which they gain greater protection for those rights retained by them. And Justice Cobb made clear that the individual keeps certain fundamental rights bestowed by natural law, even after having entered into political society:

But he is not presumed to surrender all those rights, and the public has no more right, without his consent, to invade the domain of those rights which it is necessarily to be presumed he has reserved, than he has to violate the valid regulations of the organized government under which he lives.³⁰

For Justice Cobb, then, political society was founded upon an

28. *Cf. id.* at 755 (noting that “it was not until after the *Pavesich* decision that the movement in favor of the right [to privacy] gained momentum”).

29. *Pavesich*, 50 S.E. at 69.

30. *Id.*

agreement whereby each individual freely limits certain natural rights (and concomitantly assents to the rules of the social order) in exchange for the government offering him better security for those rights that he continues to hold.

The question becomes, of course, whether the right to keep certain matters private is included in those rights provided by natural law and retained by the individual after entering the social compact. Justice Cobb viewed the answer to this question as obvious:

The right of privacy has its foundation in the instincts of nature. It is recognized intuitively, consciousness being the witness that can be called to establish its existence. Any person whose intellect is in a normal condition recognizes at once that as to each individual member of society there are matters private, and there are matters public so far as the individual is concerned. Each individual as instinctively resents any encroachment by the public upon his rights which are of a private nature as he does the withdrawal of those of his rights which are of a public nature.³¹

For this reason, Justice Cobb understood the right of privacy to derive from natural law.³² For him, it existed as a first principle, and it was not surrendered (at least not entirely) by the social compact made between the individual and society as a whole.

When viewed in this light, the right to privacy bears obvious similarities to long-held notions about rights in property. As an initial matter, Justice Cobb's explanation of the social compact is virtually identical to the theories articulated more than two centuries earlier by English philosopher John Locke. According to Locke, all persons initially are in a state of nature, that is, they are lacking organized political society.³³ In this natural state, people enjoy the freedom to decide for themselves how to arrange their affairs, including the use and disposition of their possessions and persons.³⁴ So long as individuals remain in the state of nature, however, this freedom lacks stability because every individual enjoys the exact same freedom, with none having authority to settle disputes or regulate conduct for the

31. *Id.* at 69-70.

32. *Id.* at 70-80.

33. JOHN LOCKE, SECOND TREATISE OF GOVERNMENT § 4, at 8 (C.B. Macpherson ed., Hackett Publishing Co. 1980) (1690).

34. *Id.*

mutual benefit of all.³⁵ Accordingly, the rights enjoyed in the state of nature are to some degree indefinite because they are “constantly exposed to the invasion of others.”³⁶ To obtain greater security for these rights, people unite together “for the mutual *preservation* of their lives, liberties and estates,” which Locke calls “by the general name, *property*.³⁷ Thus, for Locke, the primary purpose for which individuals create and submit to formal government “*is the preservation of their property.*”³⁸ The parallels between Locke’s theory and Justice Cobb’s discussion in *Pavesich* are striking. For both, political society results from individual desire to better protect those rights (whether property or privacy) enjoyed by the laws of nature.

At the time *Pavesich* was written, these ideas enjoyed a long pedigree in American legal thought, especially as applied to property rights.³⁹ Perhaps of primary importance were the Georgia decisions that presumably would have influenced Justice Cobb’s thinking most directly. The law of eminent domain, for example, was often explained by reference to the social compact, pointing out that the individual tacitly agrees (when necessary for the common good) to release his property for public use, but only where the government upholds its tacit agreement to provide just compensation for the taking.⁴⁰ “All property is a pledge to pay the necessary expenses of government,” said one Georgia court, “but the burthen must be equally born.”⁴¹ Thus, when the public good mandates the yielding of individual property interests, those interests

35. *Id.* § 4, at 8; *see also id.* § 123, at 66.

36. *Id.* § 123, at 66.

37. *Id.* (emphases in original).

38. *Id.* § 124, at 66 (emphasis in original).

39. *See, e.g., Vanhorne’s Lessee v. Dorrance*, 2 U.S. (2 Dall.) 304, 310 (C.C.D. Pa. 1795) (Paterson, Circuit Justice) (echoing Locke that “preservation of property . . . is a primary object of the social compact”); *Crenshaw v. Slate River Co.*, 27 Va. (6 Rand.) 245, 276 (1828) (Green, J.) (stating that “security of private property . . . is one of the primary objects of Civil Government”).

40. *See, e.g., Parham v. Justices of Inferior Court*, 9 Ga. 341, 344 (1851); *see also Heard v. Callaway*, 51 Ga. 314, 318 (1874) (“[I]t is contrary to reason and justice, *and to the fundamental principles of the social compact*, to take one man’s property and give it to another without compensation.”) (emphasis added).

41. *Parham*, 9 Ga. at 352.

nonetheless receive protection in the form of remuneration to the owner. This was so, said the Georgia courts, by virtue of the social compact itself, even where no piece of positive legislation expressly required it.⁴² As explained in another context, “independently of written constitutions, there are restrictions upon the legislative power, growing out of the nature of the civil compact and the natural rights of man.”⁴³

These brief examples demonstrate that, by 1905, social compact theory had long been associated with the law pertaining to an individual’s rights in property. A leading reason for this association, as explained by an early Justice of the United States Supreme Court, was because “[n]o man would become a member of a community, in which he could not enjoy the fruits of his honest labour and industry.”⁴⁴ This idea, too, was Lockean in nature. Just as Locke identified the social compact with the preservation of individual property interests, he identified property primarily with an individual’s personhood and labor. Locke asserted that “every man has a *property* in his own *person*,” which “no body has any right to but himself” and which includes “[t]he labour of his body, and the works of his hands.”⁴⁵ Thus, by laboring, an individual extends the scope of his property beyond himself to reach the things he produces: “Whatsoever then he removes out of the state that nature hath provided, and left it in, he hath mixed his *labour* with, and joined to it something that is his own, and thereby makes it his *property*.⁴⁶ From the individual’s vantage point, the social compact is designed primarily to safeguard both those interests he already has and those interests he might acquire, via his labor, in the future.⁴⁷

A similar rationale is implicit in Justice Cobb’s promotion of privacy rights. The notion that an individual possesses a property interest in her person and labor logically leads to the conclusion that she has some right to be protected from interference by others – that is, to be let alone. With regard to

42. *Id.* at 344-345; *Young v. McKenzie*, 3 Ga. 31, 41-42 (1847).

43. *Campbell v. State*, 11 Ga. 353, 369 (1852).

44. *Vanhorne’s Lessee v. Dorrance*, 2 U.S. (2 Dall.) 304, 310 (C.C.D. Pa. 1795) (Paterson, Circuit Justice).

45. LOCKE, *supra* note 33, § 27, at 19.

46. *Id.* (emphases in original).

47. *Id.* §§ 123-124, at 66.

the person itself, Locke's ideas "are inextricably linked to the protection of privacy, because they suppose the ability to exclude others from bodily invasion, suggesting that protection of bodily privacy also involves a metaphor for ownership itself."⁴⁸ Moreover, Locke's theory suggests that an individual might also possess some right in her own thoughts, affairs, and personal information. In fact, one scholar has described Locke's ideas as "the backbone of intellectual property law," which protects "the individual who mixes her unique personality with ideas, who most displays originality and novelty in her creations."⁴⁹ It was in this area of the law that Warren and Brandeis found their best analogy for a right to privacy.⁵⁰ This makes sense when one thinks in Lockean terms: "[I]ntellectual property embodies Locke's idea that one gains a property right in something when it emanates from one's self."⁵¹ Thus understood, privacy (as an extension of one's personhood) plays a very similar (if not identical) role to that of property with regard to the nature of the social compact. Indeed, *Pavesich* implied as much when it equated encroachments upon an individual's privacy with the withdrawal of basic societal benefits – that is, those benefits that induce the individual to enter into the social compact in the first place.⁵² If entering political society necessarily meant that each individual forfeited her right to keep certain matters private, Justice Cobb seemed to be suggesting that no one would do it.

Although *Pavesich* does not make it explicit, it seems that it is this similarity between property and privacy – the relative value of each vis-à-vis the reasons for becoming a party to the social compact – that (in the minds of Georgia jurists) linked them together as deserving of legal protection. In this line of thinking, individuals surrender certain rights (including in some instances aspects of their rights to property and privacy) in order to provide more stable and effective protection for their rights as a whole. Chief among the rights retained, and for which

48. Katyal, *supra* note 8, at 303.

49. Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1112 (2002).

50. Warren & Brandeis, *supra* note 2, at 205.

51. Solove, *supra* note 49, at 1112.

52. *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68, 69-70 (Ga. 1905).

protection is sought, are the bulk of each individual's property and privacy interests. Unless these interests receive protection, the social compact is violated and stands worthless to the individual. For this reason, at least in Georgia, both property and privacy were viewed early on as fundamental rights worthy of recognition by any civilized society.⁵³

53. *Id.* at 80 (explaining that protection of privacy rights is "thoroughly in accord . . . with the principles of the law of every civilized nation"); *In re Flournoy*, 1 Ga. 606, 608 (1846) (declaring legal protections for vested property rights "to occupy a place in the estimation of civilized states, anterior to, and above, constitutions and laws").

C. “The Bundle of Sticks” and “The Right to be Let Alone”

This similarity between privacy and property finds equal support in the final thread of *Pavesich*’s reasoning. After connecting privacy to Blackstone’s conception of fundamental rights, Justice Cobb focused his attention on providing common law support for “a legal right to be let alone.”⁷⁹ Although a

79. *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68, 71 (Ga. 1905) (internal quotations omitted).

surface reading of this portion of *Pavesich* might suggest that property and privacy share little in common, a closer review demonstrates that, in fact, Justice Cobb's argument in support of a privacy right overflows with themes and language familiar to the law of property.

Justice Cobb relied primarily on three common law examples in support of the "right to be let alone." The first and second both were found in the common law of nuisance—specifically, the enjoining of noises under the law relating to private nuisance and the punishment of a common scold, which the common law treated as a public nuisance. For Justice Cobb, the enjoining of noises (even those associated with lawful occupations) that interfere with an individual's enjoyment of his home presented "a conspicuous instance" of the law's protection of privacy.⁸⁰ With regard to such interferences, Justice Cobb indicated that "there is really no injury to the property, and the gist of the wrong is that the individual is disturbed in his right to have quiet."⁸¹ So, too, the case of the common scold or gossip. "[T]he reason for the punishment of such a character," wrote Justice Cobb, "was not the protection of any property right of her neighbors, but the fact that her conduct was a disturbance of their right to quiet and repose . . ."⁸² As his third example, Justice Cobb pointed to the common law right of persons to be secure from unreasonable searches and seizures, in which he found implicit recognition for privacy rights: "[T]he law on the subject . . . cannot be based upon any other principle than the right of a person to be secure from invasion by the public into matters of a private nature, which can only be properly termed his right of privacy."⁸³

80. *Id.*

81. *Id.*

82. *Id.*

83. *Id.* at 71-72.

Indeed, a closer look at *Pavesich* reveals that privacy's "right to be let alone" shares much in common with the figurative "bundle of sticks" that characterizes our concept of property. Although in places, *Pavesich* appeared to reject the idea that property theory provides a basis for the right of privacy, other portions of the opinion clearly suggested otherwise. Perhaps the most striking example occurred in connection with Justice Cobb's discussion of the New York case of *Roberson v. Rochester Folding Box Co.* After criticizing the majority's failure to recognize a right of privacy in that case, Justice Cobb quoted extensively from the dissenting opinion in *Roberson*, which itself was rife with property-based language.⁹² First, the *Roberson* dissent rooted the right of privacy in an individual's entitlement "to be protected in the exclusive use and enjoyment of that which is his own,"⁹³ language that has obvious similarities to the conception of property as an amalgam of rights relating to one's exclusive use and possession of a particular thing. Second, the *Roberson* dissent repeatedly noted the commercial context of that case, which (like *Pavesich*) arose from the defendant's unauthorized use of the plaintiff's likeness in advertisements for the defendant's product.⁹⁴ Implicit in this discussion was the idea that the plaintiff (and she only) had the ability to profit from her likeness, suggesting that she also possessed the exclusive right to alienate or otherwise transfer that ability. Finally, and most obviously, the *Roberson* dissent directly equated property and privacy as flowing from analogous ideas:

92. *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68, 78-79 (Ga. 1905).

93. *Roberson v. Rochester Folding Box Co.*, 64 N.E. 442, 561 (N.Y. 1902) (Gray, J., dissenting). This portion of Judge Gray's dissent was quoted in *Pavesich*, 50 S.E. at 78.

94. *Roberson*, 64 N.E. at 563-64, 566 (Gray, J., dissenting). These portions of Judge Gray's dissent were quoted in *Pavesich*, 50 S.E. at 78-79.

Property is not, necessarily, the thing itself which is owned; it is the right of the owner in relation to it. The right to be protected in one's possession of a thing or in one's privileges, belonging to him as an individual, or secured to him as a member of the commonwealth, is property, and as such entitled to the protection of the law. . . . It seems to me that the principle which is applicable is analogous to that upon which courts of equity have interfered to protect the right of privacy in cases of private writings, or of other unpublished products of the mind.⁹⁵

Not only did *Pavesich* quote all of these statements, what's more, it explicitly adopted the reasoning of the *Roberson* dissent as its own.⁹⁶

95. *Roberson*, 64 N.E. at 564 (Gray, J., dissenting). This portion of Judge Gray's was quoted in *Pavesich*, 50 S.E. at 78-79.

96. *Pavesich*, 50 S.E. at 79.

KLAYMAN et al., Plaintiffs,

v.

OBAMA et al., Defendants.

Klayman et al., Plaintiff,

v.

Obama et al., Defendants.

Civil Action No. 13-0851 (RJL)

United States District Court,
District of Columbia.

Filed December 16, 2013

Background: Subscribers to certain telecommunications and Internet services brought actions against federal government and private service providers and their executive officers, challenging the constitutionality and statutory authorization of certain of government's intelligence-gathering practices relating to wholesale collection of phone record metadata for United States citizens and analysis of that data through National Security Administration (NSA). Subscribers moved for preliminary injunction to bar government from continuing to engage in bulk collection and querying of phone record metadata, and to require government to destroy any such metadata in its possession.

Holdings: The District Court, Richard J. Leon, J., held that:

- (1) court was barred from reviewing subscribers' claim that program exceeded government's statutory authority, in violation of Administrative Procedure Act (APA);
- (2) subscribers had standing to raise Fourth Amendment challenge to collection and querying components of program;
- (3) program constituted search under Fourth Amendment;
- (4) subscribers were likely to succeed in showing that government's searches

and NSA's analysis were unreasonable under Fourth Amendment;

- (5) subscribers demonstrated irreparable harm and public interest to support injunctive relief; and
- (6) order would be stayed pending appeal, in light of national security interests and novelty of constitutional issues.

Motions granted in part and denied in part, and order stayed pending appeal.

BACKGROUND

On June 5, 2013, the British newspaper *The Guardian* reported the first of several “leaks” of classified material from Edward Snowden, a former NSA contract employee, which have revealed—and continue to reveal—multiple U.S. government intelligence collection and surveillance programs. See Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, GUARDIAN (London), June 5, 2013.⁸ That initial media report disclosed a FISC order dated April 25, 2013, compelling Verizon Business Network Services to produce to the NSA on “an ongoing daily basis . . . all call detail records or ‘telephony metadata’ created by Verizon for communications (i)

between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.” Secondary Order, *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc. d/b/a Verizon Business Services*, No. BR 13-80 at 2 (FISC Apr. 25, 2013) (attached as Ex. F to Gilligan Decl.) [Dkt. # 25-7] (“Apr. 25, 2013 Secondary Order”). According to the news article, this order “show[ed] . . . that under the Obama administration the communication records of millions of US citizens are being collected indiscriminately and in bulk—regardless of whether they are suspected of any wrongdoing.” Greenwald, *supra*. In response to this disclosure, the Government confirmed the authenticity of the April 25, 2013 FISC Order, and, in this litigation and in certain public statements, acknowledged the existence of a “program” under which “the FBI obtains orders from the FISC pursuant to Section 215 [of the USA PATRIOT Act] directing certain telecommunications service providers to produce to the NSA on a daily basis electronic copies of ‘call detail records.’” Govt.’s Opp’n at 8.⁹

⁸. Available at <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.

⁹. Although aspects of the program remain classified, including which other telecommunications service providers besides Verizon Business Network Services are involved, the Government has declassified and made available to the public certain facts about the program. See Office of the Dir. of Nat'l Intelligence, *DNI Statement on Recent Unauthorized Disclosure of Classified Information* (June 6, 2013), available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information>; Office of the Dir. of Nat'l Intelligence, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)* (Sept. 10, 2013), available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document>; Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT Act (Aug. 9, 2013), available at <http://apps.washingtonpost.com/g/page/politics/obama-administration-white-paper-on-nsa-surveillance-oversight/388/>.

lection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA) (Aug. 21, 2013), available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa>; Office of the Dir. of Nat'l Intelligence, *DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)* (Sept. 10, 2013), available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document>; Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT Act (Aug. 9, 2013), available at <http://apps.washingtonpost.com/g/page/politics/obama-administration-white-paper-on-nsa-surveillance-oversight/388/>.

Follow-on media reports revealed other Government surveillance programs, including the Government's collection of internet data pursuant to a program called "PRISM." See Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps into user data of Apple, Google and others*, GUARDIAN (London), June 6, 2013.¹⁰

Soon after the first public revelations in the news media, plaintiffs filed their complaints in these two cases on June 6, 2013 (*Klayman I*) and June 12, 2013 (*Klayman II*), alleging that the Government, with the participation of private companies, is conducting "a secret and illegal government scheme to intercept and analyze vast quantities of domestic telephonic communications," Second Am. Compl. ¶ 2 (*Klayman I*), and "of communications from the Internet and electronic service providers," Am. Compl. ¶ 2 (*Klayman II*). Plaintiffs in *Klayman I*—attorney Larry Klayman, founder of Freedom Watch, a public interest organization, and Charles Strange, the father of Michael Strange, a cryptologist technician for the NSA and support personnel for Navy SEAL Team VI who was killed in Afghanistan when his helicopter was shot down in 2011—assert that they are subscribers of Verizon Wireless and bring suit against the NSA, the Department of Justice ("DOJ"), and several executive officials (President Barack H. Obama, Attorney General Eric H. Holder, Jr., General Keith B. Alexander, Director of the NSA, and U.S. District Judge Roger Vinson), as well as Verizon Communications and its chief executive officer. Second Am. Compl. ¶¶ 9–19; Klayman Aff. ¶ 3; Strange Aff. ¶ 2. And plaintiffs in *Klayman II*—Mr. Klayman and Mr. Strange again, along with two private in-

vestigators, Michael Ferrari and Matthew Garrison—bring suit against the same Government defendants, as well as Facebook, Yahoo!, Google, Microsoft, YouTube, AOL, PalTalk, Skype, Sprint, AT & T, and Apple, asserting that plaintiffs are "subscribers, users, customers, and otherwise avail themselves to" these named internet and/or telephone service provider companies. Am. Compl. ¶¶ 1, 11–14; Klayman Aff. ¶ 3; Klayman Suppl. Aff. ¶ 3; Strange Aff. ¶ 3.¹¹ Specifically, plaintiffs allege that the Government has violated their individual rights under the First, Fourth, and Fifth Amendments of the Constitution and has violated the Administrative Procedure Act ("APA") by exceeding its statutory authority under FISA.¹² Second Am. Compl. ¶¶ 1–8, 49–99.

I. Statutory Background

A. FISA and Section 215 of the USA PATRIOT Act (50 U.S.C. § 1861)

In 1978, Congress enacted the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 *et seq.* ("FISA"), "to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes." *Clapper v. Amnesty Int'l USA*, — U.S. —, 133 S.Ct. 1138, 1143, 185 L.Ed.2d 264 (2013). Against the backdrop of findings by the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the "Church Committee") that the executive branch had, for decades, engaged in warrantless domestic intelligence-gathering activities that had illegally infringed the Fourth Amendment rights of American citizens, Congress passed FISA

10. Available at <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

11. See *supra*, notes 5, 6.

12. Plaintiffs also allege certain statutory violations by the private company defendants, Sec-

ond Am. Compl. ¶¶ 81–95, which are not at issue for purposes of the Preliminary Injunction Motions, as well as common law privacy tort claims, Second Am. Compl. ¶¶ 70–80.

“in large measure [as] a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused.” S.Rep. No. 95–604, at 7. In the view of the Senate Judiciary Committee, the act went “a long way in striking a fair and just balance between protection of national security and protection of personal liberties.” *Id.* at 7.

FISA created a procedure for the Government to obtain ex parte judicial orders authorizing domestic electronic surveillance upon a showing that, *inter alia*, the target of the surveillance was a foreign power or an agent of a foreign power. 50 U.S.C. §§ 1804(a)(3), 1805(a)(2). In enacting FISA, Congress also created two new Article III courts—the Foreign Intelligence Surveillance Court (“FISC”), composed of eleven U.S. district judges, “which shall have jurisdiction to hear applications for and grant orders approving” such surveillance, § 1803(a)(1), and the FISC Court of Review, composed of three U.S. district or court of appeals judges, “which shall have jurisdiction to review the denial of any application made under [FISA],” § 1803(b).¹³

In addition to authorizing wiretaps, §§ 1801–1812, FISA was subsequently amended to add provisions enabling the Government to obtain ex parte orders au-

13. The eleven U.S. district judges are appointed by the Chief Justice of the United States to serve on the FISC for a term of seven years each. 50 U.S.C. § 1803(a)(1), (d). They are drawn from at least seven of the twelve judicial circuits in the United States, and at least three of the judges must reside within twenty miles of the District of Columbia. § 1803(a)(1). For these eleven district judges who comprise the FISC at any one time, their service on the FISC is *in addition to*, not in lieu of, their normal judicial duties in the districts in which they have been appointed. See Theodore W. Ruger, *Chief Justice Rehnquist’s Appointments to the FISA Court: An Empirical Perspective*, 101 Nw. U.L. REV. 239, 244 (2007) (“Service on the FISA Court is a

thorizing physical searches, §§ 1821–1829, as well as pen registers and trap-and-trace devices, §§ 1841–1846. See Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103–359, § 807(a)(3), 108 Stat. 3423; Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105–272, § 601(2), 112 Stat. 2396 (“1999 Act”). In 1998, Congress added a “business records” provision to FISA. See 1999 Act § 602. Under that provision, the FBI was permitted to apply for an ex parte order authorizing specified entities, such as common carriers, to release to the FBI copies of business records upon a showing in the FBI’s application that “there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.” 50 U.S.C. § 1862(b)(2)(B) (2000).

Following the September 11, 2001 terrorist attacks, Congress passed the USA PATRIOT Act, which made changes to FISA and several other laws. Pub. L. No. 107–56, 115 Stat. 272 (2001). Section 215 of the PATRIOT Act replaced FISA’s business-records provision with a more expansive “tangible things” provision. Codified at 50 U.S.C. § 1861, it authorizes the FBI to apply “for an order requiring the production of any tangible things (includ-

part-time position. The judges rotate through the court periodically and maintain regular district court caseloads in their home courts.”). Accordingly, service on the FISC is, at best, a part-time assignment that occupies a relatively small part of each judge’s annual judicial duties. Further, as a result of the requirement that at least three judges reside within twenty miles of the nation’s capital, a disproportionate number of the FISC judges are drawn from the district courts of the District of Columbia and the Eastern District of Virginia, *see id.* at 258 (Appendix) (listing Chief Justice Rehnquist’s twenty-five appointments to the FISC, six of which came from the D.D.C. and E.D. Va.).

ing books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.” § 1861(a)(1). While this provision originally required that the FBI’s application “shall specify that the records concerned are sought for” such an investigation, § 1861(b)(2) (Supp. I 2001), Congress amended the statute in 2006 to provide that the FBI’s application must include “a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.” § 1861(b)(2)(A); *see USA PATRIOT Improvement and Reauthorization Act of 2005*, Pub. L. No. 109–177, § 106(b), 120 Stat. 192 (“USA PATRIOT Improvement and Reauthorization Act”).

Section 1861 also imposes other requirements on the FBI when seeking to use this authority. For example, the investigation pursuant to which the request is made must be authorized and conducted under guidelines approved by the Attorney General under Executive Order No. 12,333 (or a successor thereto). 50 U.S.C. § 1861(a)(2)(A), (b)(2)(A). And the FBI’s application must “enumerat[e] . . . minimization procedures adopted by the Attorney General . . . that are applicable to the retention and dissemination by the [FBI] of any tangible things to be made available to the [FBI] based on the order requested.” § 1861(b)(2)(B). The statute defines “minimization procedures” as, in relevant part, “specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpub-

licly available information concerning unconsenting [U.S.] persons consistent with the need of the [U.S.] to obtain, produce, and disseminate foreign intelligence information.” § 1861(g)(2). If the FISC judge finds that the FBI’s application meets these requirements, he “shall enter an ex parte order as requested, or as modified, approving the release of tangible things” (hereinafter, “production order”). § 1861(c)(1); *see also* § 1861(f)(1)(A) (“the term ‘production order’ means an order to produce any tangible thing under this section”).

Under Section 1861’s “use” provision, information that the FBI acquires through such a production order “concerning any [U.S.] person may be used and disclosed by Federal officers and employees without the consent of the [U.S.] person only in accordance with the minimization procedures adopted” by the Attorney General and approved by the FISC. § 1861(h). Meanwhile, recipients of Section 1861 production orders are obligated not to disclose the existence of the orders, with limited exceptions. § 1861(d)(1).

B. Judicial Review by the FISC

While the recipient of a production order must keep it secret, Section 1861 does provide the recipient—but only the recipient—a right of judicial review of the order before the FISC pursuant to specific procedures. Prior to 2006, recipients of Section 1861 production orders had no express right to judicial review of those orders, but Congress added such a provision when it reauthorized the PATRIOT Act that year. *See USA PATRIOT Improvement and Reauthorization Act* § 106(f); 1 D. KRIS & J. WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 19:7 (2d ed. 2012) (“Kris & Wilson”) (“Prior to the Reauthorization Act in 2006, FISA did not allow for two-party litigation before the FISC”).

Under Section 1861, “[a] person receiving a production order may challenge the legality of that order by filing a petition with the [petition review pool of FISC judges].” 50 U.S.C. § 1861(f)(2)(A)(i); *see* § 1803(e)(1).¹⁴ The FISC review pool judge considering the petition may grant the petition “only if the judge finds that [the] order does not meet the requirements of [Section 1861] or is otherwise unlawful.” § 1861(f)(2)(B). Once the FISC review pool judge rules on the petition, either the Government or the recipient of the production order may seek an en banc hearing before the full FISC, § 1803(a)(2)(A), or may appeal the decision by filing a petition for review with the FISC Court of Review, § 1861(f)(3). Finally, after the FISC Court of Review renders a written decision, either the Government or the recipient of the production order may then appeal this decision to the Supreme Court on petition for writ of certiorari. §§ 1861(f)(3), 1803(b). A production order “not explicitly modified or set aside consistent with [Section 1861(f)] shall remain in full effect.” § 1861(f)(2)(D).

Consistent with other confidentiality provisions of FISA, Section 1861 provides that “[a]ll petitions under this subsection shall be filed under seal,” § 1861(f)(5), and the “record of proceedings . . . shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence,” § 1861(f)(4). *See also* § 1803(c).

14. The three judges who reside within twenty miles of the District of Columbia comprise the petition review pool (unless all three are unavailable, in which case other FISC judges may be designated). § 1803(e)(1). In addition to reviewing petitions to review Section 1861 production orders pursuant to § 1861(f), the review pool also has jurisdiction to review petitions filed pursuant to § 1881a(h)(4). *Id.*

15. In addition to alleging that the NSA has “direct access” to Verizon’s databases, Sec-

II. Collection of Bulk Telephony Metadata Pursuant to Section 1861

To say the least, plaintiffs and the Government have portrayed the scope of the Government’s surveillance activities very differently.¹⁵ For purposes of resolving these preliminary injunction motions, however, as will be made clear in the discussion below, it will suffice to accept the Government’s description of the phone metadata collection and querying program. *Cf. Cobell v. Norton*, 391 F.3d 251, 261 (D.C.Cir.2004) (evidentiary hearing on preliminary injunction is necessary only if the court must make credibility determinations to resolve key factual disputes in favor of the *moving party*).

In broad overview, the Government has developed a “counterterrorism program” under Section 1861 in which it collects, compiles, retains, and analyzes certain telephone records, which it characterizes as “business records” created by certain telecommunications companies (the “Bulk Telephony Metadata Program”). The records collected under this program consist of “metadata,” such as information about what phone numbers were used to make and receive calls, when the calls took place, and how long the calls lasted. Decl. of Acting Assistant Director Robert J. Holley, Federal Bureau of Investigation (“Holley Decl.”) [Dkt. # 25–5], at ¶ 5; Decl. of Teresa H. Shea, Signals Intelligence Director, National Security Agency (“Shea Decl.”) [Dkt. # 25–4], at ¶ 7; Primary Or-

ond Am. Compl. ¶ 7, and is collecting location information as part of “call detail records,” Pls. Mem. at 10, Mr. Klayman and Mr. Strange also suggest that they are “prime target[s]” of the Government due to their public advocacy and claim that the Government is behind alleged inexplicable text messages being sent from and received on their phones, Pls.’ Mem. at 13–16; Klayman Aff. ¶ 11; Strange Aff. ¶¶ 12–17.

der, *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things From [Redacted]*, No. BR 13-158 at 3 n.1 (FISC Oct. 11, 2013) (attached as Ex. B to Gilligan Decl.) [Dkt. # 25-3] (“Oct. 11, 2013 Primary Order”).¹⁶ According to the representations made by the Government, the metadata records collected under the program do *not* include *any* information about the content of those calls, or the names, addresses, or financial information of any party to the calls. Holley Decl. ¶¶ 5, 7; Shea Decl. ¶ 15; Oct. 11, 2013 Primary Order at 3 n.1.¹⁷ Through targeted computerized searches of those metadata records, the NSA tries to discern connections between terrorist organizations and previously unknown terrorist operatives located in the United States. Holley Decl. ¶ 5; Shea Decl. ¶¶ 8–10, 44.

The Government has conducted the Bulk Telephony Metadata Program for more than seven years. Beginning in May 2006 and continuing through the present,¹⁸ the FBI has obtained production orders from the FISC under Section 1861 directing certain telecommunications companies

to produce, on an ongoing daily basis, these telephony metadata records, Holley Decl. 16; Shea Decl. ¶ 13, which the companies create and maintain as part of their business of providing telecommunications services to customers, Holley Decl. ¶ 10; Shea Decl. ¶ 18. The NSA then consolidates the metadata records provided by different telecommunications companies into one database, Shea Decl. ¶ 23, and under the FISC’s orders, the NSA may retain the records for up to five years, *id.* ¶ 30; *see* Oct. 11, 2013 Primary Order at 14. According to Government officials, this aggregation of records into a single database creates “an historical repository that permits retrospective analysis,” Govt.’s Opp’n at 12, enabling NSA analysts to draw connections, across telecommunications service providers, between numbers reasonably suspected to be associated with terrorist activity and with other, unknown numbers. Holley Decl. ¶¶ 5, 8; Shea Decl. ¶¶ 46, 60.

The FISC orders governing the Bulk Telephony Metadata Program specifically provide that the metadata records may be

16. Oct. 11, 2013 Primary Order at 3 n.1 (“For purposes of this Order ‘telephony metadata’ includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call”).

17. Plaintiffs have alleged that the Government has also collected location information* for cell phones. Second Am. Comp. ¶ 28; Pls.’ Mem. at 10–11. While more recent FISC opinions expressly state that cell-site location information is not covered by Section 1861 production orders, *see, e.g.*, Oct. 11, 2013 Primary Order at 3 n.1, the Government has *not* affirmatively represented to this Court that the NSA has *not*, at any point in the history of the Bulk Telephony Metadata Pro-

gram, collected location information (in one technical format or another) about cell phones. *See, e.g.*, Govt.’s Opp’n at 9 (defining telephony metadata and noting what is not included); Order, *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 06-05 at 2 (FISC May 24, 2006), available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document> (defining telephony metadata and noting what is not included, but *not* expressly stating that the order does *not* authorize the production of cell-site location information).

18. The most recent FISC order authorizing the Bulk Telephony Metadata Program that the Government has disclosed (in redacted form, directed to an unknown recipient) expires on January 3, 2014. *See* Oct. 11, 2013 Primary Order at 17.

accessed only for counterterrorism purposes (and technical database maintenance). Holley Decl. ¶ 8; Shea Decl. ¶ 30. Specifically, NSA intelligence analysts, *without seeking the approval of a judicial officer*, may access the records to obtain foreign intelligence information only through “queries” of the records performed using “identifiers,” such as telephone numbers, associated with terrorist activity.¹⁹ An “identifier” (i.e., selection term, or search term) used to start a query of the database is called a “seed,” and “seeds” must be approved by one of twenty-two designated officials in the NSA’s Homeland Security Analysis Center or other parts of the NSA’s Signals Intelligence Directorate. Shea Decl. ¶¶ 19, 31. Such approval may be given only upon a determination by one of those designated officials that there exist facts giving rise to a “reasonable, articulable suspicion” (“RAS”) that the selection term to be queried is associated with one or more of the specified foreign terrorist organizations approved for targeting by the FISC. Holley Decl. ¶¶ 15–16.²⁰ In 2012, for example, fewer than 300 unique identifiers met this RAS standard and were used as “seeds” to query the metadata, but “the number of unique identifiers has varied over the years.” Shea Decl. ¶ 24.

When an NSA intelligence analyst runs a query using a “seed,” the minimization procedures provide that query results are

19. In her declaration, Teresa H. Shea, Director of the Signals Intelligence Directorate at the NSA, states that “queries,” or “term searches,” of the metadata database are conducted “using metadata ‘identifiers,’ e.g., *telephone numbers*, that are associated with a foreign terrorist organization.” Shea Decl. ¶ 19 (emphasis added). If a telephone number is only an *example* of an identifier that may be used as a search term, it is not clear what other “identifiers” may be used to query the database, and the Government has not elaborated. *See, e.g.*, Oct. 11, 2013 Primary

limited to records of communications within three “hops” from the seed. *Id.* ¶ 22. The query results thus will include only identifiers and their associated metadata having a direct contact with the seed (the first “hop”), identifiers and associated metadata having a direct contact with first “hop” identifiers (the second “hop”), and identifiers and associated metadata having a direct contact with second “hop” identifiers (the third “hop”). *Id.* ¶ 22; Govt.’s Opp’n at 11. In plain English, this means that if a search starts with telephone number (123) 456-7890 as the “seed,” the first hop will include all the phone numbers that (123) 456-7890 has called or received calls from in the last five years (say, 100 numbers), the second hop will include all the phone numbers that each of *those* 100 numbers has called or received calls from in the last five years (say, 100 numbers for each one of the 100 “first hop” numbers, or 10,000 total), and the third hop will include all the phone numbers that each of *those* 10,000 numbers has called or received calls from in the last five years (say, 100 numbers for each one of the 10,000 “second hop” numbers, or 1,000,000 total). *See* Shea Decl. ¶ 25 n.1. The actual number of telephone numbers and their associated metadata captured in any given query varies, of course, but in the absence of any specific representations from the Government about typical query results, it is likely that the quantity of phone numbers captured in any given query would be very large.²¹

Order at 5 n.4, 7–10 (redacting text that appears to discuss “selection terms”).

20. A determination that a selection term meets the RAS standard remains effective for 180 days for any selection term reasonably believed to be used by a U.S. person, and for one year for all other selection terms. *See* Oct. 11, 2013 Primary Order at 10.

21. After stating that fewer than 300 unique identifiers met the RAS standard and were used as “seeds” to query the metadata in 2012, Ms. Shea notes that “[b]ecause the

Once a query is conducted and it returns a universe of responsive records (i.e., a universe limited to records of communications within three hops from the seed), trained NSA analysts may then perform new searches and otherwise perform intelligence analysis *within* that universe of data without using RAS-approved search terms. See Shea Decl. ¶ 26 (NSA analysts may “chain contacts within the query results themselves”); Oct. 11, 2013 Primary

same seed identifier can be queried more than once over time, can generate multiple responsive records, and can be used to obtain contact numbers up to three ‘hops’ from the seed identifier, the number of metadata records responsive to such queries is *substantially larger than 300, but is still a very small percentage of the total volume of metadata records.*” Shea Decl. ¶ 24 (emphasis added). The first part of this assertion is a glaring understatement, while the second part is virtually meaningless when placed in context. First, as the sample numbers I have used in the text above demonstrate, it is possible to arrive at a query result in the millions within three hops while using even conservative numbers—needless to say, this is “substantially larger than 300.” After all, even if the average person in the United States does not call or receive calls from 100 unique phone numbers in one year, what about over a five-year period? And second, it belabors the obvious to note that even a few million phone numbers is “a very small percentage of the total volume of metadata records” if the Government has collected metadata records on hundreds of millions of phone numbers.

But it’s also easy to imagine the spiderweb-like reach of the three-hop search growing exponentially and capturing even higher numbers of phone numbers. Suppose, for instance, that there is a person living in New York City who has a phone number that meets the RAS standard and is approved as a “seed.” And suppose this person, who may or may not actually be associated with any terrorist organization, calls or receives calls from 100 unique numbers, as in my example. But now suppose that one of the numbers he calls is his neighborhood Domino’s Pizza shop. The Court won’t hazard a guess as to how many different phone numbers might dial a given Domino’s Pizza outlet in New York City in a five-year period, but to take a

Order.²² According to the Government, following the “chains of communication”—which, for chains that cross different communications networks, is only possible if the metadata is aggregated—allows the analyst to discover information that may not be readily ascertainable through other, targeted intelligence-gathering techniques. Shea Decl. ¶ 46. For example, the query might reveal that a seed telephone number

page from the Government’s book of understatement, it’s “substantially larger” than the 100 in the second hop of my example, and would therefore most likely result in exponential growth in the scope of the query and lead to millions of records being captured by the third hop. (I recognize that some minimization procedures described in recent FISC orders permitting technical personnel to access the metadata database to “defeat [] high volume and other unwanted [] metadata,” Oct. 11, 2013 Primary Order at 6, may, in practice, reduce the likelihood of my Domino’s hypothetical example occurring. But, of course, that does not change the baseline fact that, by the terms of the FISC’s orders, the NSA is permitted to run queries capturing up to three hops that can conceivably capture millions of Americans’ phone records. Further, these queries using non-RAS-approved selection terms, which are permitted to make the database “usable for intelligence analysis,” *id.* at 5, may very well themselves involve searching across millions of records.)

22. Under the terms of the most recent FISC production order available, “[q]ueries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below. This automated query process queries the collected BR metadata (in a ‘collection store’) with RAS-approved selection terms and returns the hop-limited results from those queries to a ‘corporate store.’ The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms.” Oct. 11, 2013 Primary Order at 11 (footnote omitted). This “automated query process” was first approved by the FISC in a November 8, 2012 order. *Id.* at 11 n.11.

has been in contact with a previously unknown U.S. telephone number—i.e., on the first hop. *See id.* ¶58. And from there, “contact-chaining” out to the second and third hops to examine the contacts made by that telephone number may reveal a contact with other telephone numbers already known to the Government to be associated with a foreign terrorist organization. *Id.* ¶¶ 47, 62. In short, the Bulk Telephony Metadata Program is meant to detect: (1) domestic U.S. phone numbers calling *outside* of the U.S. to foreign phone numbers associated with terrorist groups; (2) foreign phone numbers associated with terrorist groups calling *into* the U.S. to U.S. phone numbers; and (3) “possible terrorist-related communications” between U.S. phone numbers *inside* the U.S. *See id.* ¶44.

Since the program began in May 2006, the FISC has repeatedly approved applications under Section 1861 and issued orders directing telecommunications service providers to produce records in connection with the Bulk Telephony Metadata Program. Shea Decl. ¶¶ 13–14. Through October 2013, fifteen different FISC judges have issued thirty-five orders authorizing the program. Govt.’s Opp’n at 9; *see also* Shea Decl. ¶¶ 13–14; Holley Decl. ¶6. Under those orders, the Government must periodically seek renewal of the authority to collect telephony records (typically ev-

23. Judge Walton noted that, “since the earliest days of the FISC-authorized collection of call-detail records by the NSA, the NSA has on a daily basis, accessed the BR metadata for purposes of comparing thousands of non-RAS-approved telephone identifiers on its alert list against the BR metadata in order to identify any matches. Such access was prohibited by the governing minimization procedures under each of the relevant Court orders.” Mar. 2, 2009 Order, 2009 WL 9150913, at *2. He went on to conclude: “In summary, since January 15, 2009, it has finally come to light that the FISC’s authorizations of this vast collection program have been

ery ninety days). Shea Decl. ¶14. The Government has nonetheless acknowledged, as it must, that failures to comply with the minimization procedures set forth in the orders have occurred. For instance, in January 2009, the Government reported to the FISC that the NSA had improperly used an “alert list” of identifiers to search the bulk telephony metadata, which was composed of identifiers that had *not* been approved under the RAS standard. *Id.* ¶37; Order, *In re Production of Tangible Things from [Redacted]*, No. BR 08–13, 2009 WL 9150913, at *2 (FISC Mar. 2, 2009) (“Mar. 2, 2009 Order”). After reviewing the Government’s reports on its noncompliance, Judge Reggie Walton of the FISC concluded that the NSA had engaged in “systematic noncompliance” with FISC-ordered minimization procedures over the preceding three years, since the inception of the Bulk Telephony Metadata Program, and had also repeatedly made misrepresentations and inaccurate statements about the program to the FISC judges. Mar. 2, 2009 Order, 2009 WL 9150913, at *2–5.²³ As a consequence, Judge Walton concluded that he had no confidence that the Government was doing its utmost to comply with the court’s orders, and ordered the NSA to seek FISC approval on a *case-by-case basis* before conducting any further queries of the bulk telephony metadata collected pursuant to

premised on a flawed depiction of how the NSA uses BR metadata. This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government’s submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively.” *Id.* at *5.

Section 1861 orders. *Id.* at *9; Shea Decl.

¶¶ 38–39. This approval procedure remained in place from March 2009 to September 2009. Shea Decl. ¶¶ 38–39.

Notwithstanding this six-month “sanction” imposed by Judge Walton, the Government apparently has had further compliance problems relating to its collection programs in subsequent years. In October 2011, the Presiding Judge of the FISC, Judge John Bates, found that the Government had misrepresented the scope of its targeting of certain internet communications pursuant to 50 U.S.C. § 1881a (i.e., a different collection program than the Bulk Telephony Metadata Program at issue here). Referencing the 2009 compliance issue regarding the NSA’s use of unauthorized identifiers to query the metadata in the Bulk Telephony Metadata Program, Judge Bates wrote: “the Court is troubled that the government’s revelations regarding NSA’s acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.” Mem. Op., [Redacted], No. [redacted], at 16 n.14 (FISC Oct. 3, 2011).²⁴ Both Judge Walton’s and Judge Bates’s opinions were only recently declassified by the Government in response to the Congressional and public reaction to the Snowden leaks.²⁵

24. Available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa>. Whatever the second “substantial misrepresentation” was, the Government appears to have redacted it from the footnote in that opinion.

25. See Office of the Dir. of Nat’l Intelligence, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance*

Act (FISA) (Aug. 21, 2013), available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa>; Office of the Dir. of Nat’l Intelligence, *DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)* (Sept. 10, 2013), available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document>.

[17, 18] The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. CONST. amend IV. That right “shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” *Id.* A Fourth Amendment “search” occurs either when “the Govern-

ment obtains information by physically intruding on a constitutionally protected area,” *United States v. Jones*, — U.S. —, 132 S.Ct. 945, 950 n.3, 181 L.Ed.2d 911 (2012), or when “the government violates a subjective expectation of privacy that society recognizes as reasonable,” *Kyllo v. United States*, 533 U.S. 27, 33, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring)). This case obviously does not involve a physical intrusion, and plaintiffs do not claim otherwise.⁴¹

[19] The threshold issue that I must address, then, is whether plaintiffs have a reasonable expectation of privacy that is violated when the Government indiscriminately collects their telephony metadata along with the metadata of hundreds of millions of other citizens without any particularized suspicion of wrongdoing, retains all of that metadata for five years, and then queries, analyzes, and investigates that data without prior judicial approval of the investigative targets. If they do—and a Fourth Amendment search has thus occurred—then the next step of the analysis will be to determine whether such a search is “reasonable.” See *id.* at 31, 121 S.Ct. 2038 (whether a search has occurred is an “antecedent question” to whether a search was reasonable).⁴²

41. “A ‘seizure’ of property occurs when there is some meaningful interference with an individual’s possessory interests in that property.” *United States v. Jacobsen*, 466 U.S. 109, 113, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984). Plaintiffs have not offered any theory as to how they would have a possessory interest in their phone data held by Verizon, and I am aware of none.

42. While it is true “[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear,” *City of Ontario v. Quon*, 560 U.S. 746, 130 S.Ct.

i. The Collection and Analysis of Telephony Metadata Constitutes a Search.

The analysis of this threshold issue of the expectation of privacy must start with the Supreme Court’s landmark opinion in *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), which the FISC has said “squarely control[s]” when it comes to “[t]he production of telephone service provider metadata.” Am. Mem. Op., *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from [REDACTED]*, No. BR 13-109 at 6-9 (FISC Aug. 29, 2013) (attached as Ex. A to Gilligan Decl.) [Dkt. # 25-2]. In *Smith*, police were investigating a robbery victim’s reports that she had received threatening and obscene phone calls from someone claiming to be the robber. *Id.* at 737, 99 S.Ct. 2577. Without obtaining a warrant or court order, police installed a pen register, which revealed that a telephone in Smith’s home had been used to call the victim on one occasion.⁴³ *Id.* The Supreme Court held that Smith had no reasonable expectation of privacy in the numbers dialed from his phone because he voluntarily transmitted them to his phone company, and because it is generally known that phone companies keep such information in their business records. *Id.* at 742-44, 99 S.Ct. 2577. The main thrust of the Government’s argument here

2619, 2629, 177 L.Ed.2d 216 (2010), phone call and text messaging technology is not “emerging,” nor is “its role in society” unclear. I therefore believe that it is appropriate and necessary to elaborate on the Fourth Amendment implications of the NSA’s metadata collection program.

43. A “pen register” is “a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted” (i.e., it records limited data on outgoing calls). 18 U.S.C. § 3127(3).

is that under *Smith*, no one has an expectation of privacy, let alone a reasonable one, in the telephony metadata that telecom companies hold as business records; therefore, the Bulk Telephony Metadata Program is not a search. Govt.'s Opp'n at 45–50. I disagree.

The question before me is *not* the same question that the Supreme Court confronted in *Smith*. To say the least, “whether the installation and use of a pen register constitutes a ‘search’ within the meaning of the Fourth Amendment,” *id.* at 736, 99 S.Ct. 2577—under the circumstances addressed and contemplated in that case—is a far cry from the issue in this case.

Indeed, the question in this case can more properly be styled as follows: When do present-day circumstances—the evolutions in the Government’s surveillance capabilities, citizens’ phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now.

In *United States v. Jones*, — U.S. —, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012), five justices found that law enforcement’s use of a GPS device to track a vehicle’s movements for nearly a month violated Jones’s reasonable expectation of privacy. See *id.* at 955–56 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring). Significantly, the justices did so *without* questioning the validity of the

Court’s earlier decision in *United States v. Knotts*, 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983), that use of a tracking beeper does not constitute a search because “[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”⁴⁴ *Id.* at 281, 103 S.Ct. 1081. Instead, they emphasized the many significant ways in which the short-range, short-term tracking device used in *Knotts* differed from the constant month-long surveillance achieved with the GPS device attached to Jones’s car. See *Jones*, 132 S.Ct. at 956 n.* (Sotomayor, J., concurring) (*Knotts* “does not foreclose the conclusion that GPS monitoring, in the absence of a physical intrusion, is a Fourth Amendment search”); *id.* at 964 (Alito, J., concurring) (“[R]elatively short-term monitoring of a person’s movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.” (citation omitted)); see also *United States v. Maynard*, 615 F.3d 544, 557 (D.C.Cir. 2010), *aff’d sub nom. Jones*, — U.S. —, 132 S.Ct. 945, 181 L.Ed.2d 911 (“*Knotts* held only that ‘[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,’ not that such a person has no reasonable expectation of privacy in his movements whatsoever, world without end, as the Government would have it.” (citation omitted; quoting *Knotts*, 460 U.S. at 281, 103 S.Ct. 1081)).⁴⁵

44. In *Jones*, the Government relied heavily on *Knotts* (and *Smith*) as support for the argument that Jones had no expectation of privacy in his movements on the roads because he voluntarily disclosed them to the public. See generally Brief for Petitioner, *United States v. Jones*, 132 S.Ct. 945 (2012) (No. 10–1259), 2011 WL 3561881; Reply Brief for Petitioner, *United States v. Jones*, 132 S.Ct. 945 (2012)

(No. 10–1259), 2011 WL 5094951. Five justices found that argument unconvincing.

45. Lower courts, too, have recognized that the Supreme Court’s Fourth Amendment decisions cannot be read too broadly. See, e.g., *United States v. Cuevas-Sanchez*, 821 F.2d 248, 251 (5th Cir.1987) (“It does not follow that [California v. Ciraolo, 476 U.S. 207, 106

[20, 21] Just as the Court in *Knotts* did not address the kind of surveillance used to track Jones, the Court in *Smith* was not confronted with the NSA's Bulk Telephony Metadata Program.⁴⁶ Nor could the Court in 1979 have ever imagined how the citizens of 2013 would interact with their phones. For the many reasons discussed below, I am convinced that the surveillance program now before me is so different from a simple pen register that *Smith* is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search. To the contrary, for the following reasons, I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.

First, the pen register in *Smith* was operational for only a matter of days between March 6, 1976 and March 19, 1976, and there is no indication from the Court's opinion that it expected the Government to retain those limited phone records once the case was over. *See* 442 U.S. at 737, 99 S.Ct. 2577. In his affidavit, Acting Assistant Director of the FBI Robert J. Holley himself noted that "[p]en-register and trap-and-trace (PR/TT) devices provide no historical contact information, only a record of contacts with the target occurring

after the devices have been installed." Holley Decl. ¶ 9. This short-term, forward-looking (as opposed to historical), and highly-limited data collection is what the Supreme Court was assessing in *Smith*. The NSA telephony metadata program, on the other hand, involves the creation and maintenance of a historical database containing *five years'* worth of data. And I might add, there is the very real prospect that the program will go on for as long as America is combatting terrorism, which realistically could be forever!

[22] Second, the relationship between the police and the phone company in *Smith* is *nothing* compared to the relationship that has apparently evolved over the last seven years between the Government and telecom companies. Compare *Smith*, 442 U.S. at 737, 99 S.Ct. 2577 ("[T]he telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at petitioner's home."), *with* Govt.'s Opp'n at 8–9 ("Under this program, . . . certain telecommunications service providers [] produce to the NSA *on a daily basis* electronic copies of call detail records, or telephony metadata. . . . The FISC *first authorized the program in May 2006*, and since then has renewed the

S.Ct. 1809, 90 L.Ed.2d 210 (1986), which held that police did not violate a reasonable expectation of privacy when they engaged in a warrantless aerial observation of marijuana plants growing on curtilage of a home using only the naked eye from a height of 1,000 feet,] authorizes any type of surveillance whatever just because one type of minimally-intrusive aerial observation is possible.'").

46. True, the Court in *Knotts* explicitly "reserved the question whether 'different constitutional principles may be applicable' to 'dragnet-type law enforcement practices' of the type that GPS tracking made possible" in *Jones*. *Jones*, 132 S.Ct. at 952 n.6 (quoting *Knotts*, 460 U.S. at 284, 103 S.Ct. 1081); *see also id.* at 956, n.* (Sotomayor, J., concurring). That the Court in *Smith* did not explic-

itly hold open the question of whether an exponentially broader, high-tech, years-long bulk telephony metadata collection program would infringe on reasonable expectations of privacy does not mean that the Court's holding necessarily extends so far as to answer that novel question. The Supreme Court itself has recognized that prior Fourth Amendment precedents and doctrines do not always control in cases involving unique factual circumstances created by evolving technology. *See, e.g., Kyllo*, 533 U.S. at 34, 121 S.Ct. 2038 ("To withdraw protection of this minimum expectation [of privacy in the home] would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."). If this isn't such a case, then what is?

program thirty-five times" (emphases added; citation and internal quotation marks omitted)). The Supreme Court itself has long-recognized a meaningful difference between cases in which a third party collects information and then turns it over to law enforcement, *see, e.g., Smith*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220; *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976), and cases in which the government and the third party create a formalized policy under which the service provider collects information for law enforcement purposes, *see Ferguson v. Charleston*, 532 U.S. 67, 121 S.Ct. 1281, 149 L.Ed.2d 205 (2001), with the latter raising Fourth Amendment concerns. In *Smith*, the Court considered a one-time, targeted request for data regarding an individual suspect in a criminal investigation, *see Smith*, 442 U.S. at 737, 99 S.Ct. 2577, which in no way resembles the daily, all-encompassing, indiscriminate dump of phone metadata that the NSA now receives as part of its Bulk Telephony Metadata Program. It's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence-gathering operation with the Government. Cf. *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 764, 109 S.Ct. 1468, 103 L.Ed.2d 774 (1989) ("Plainly there is a vast difference between the public records that might be found after a diligent search of

47. When an individual makes his property accessible to third parties, he may still retain some expectation of privacy based on his understanding of how third parties typically handle that property. *See Bond v. United States*, 529 U.S. 334, 338–39, 120 S.Ct. 1462, 146 L.Ed.2d 365 (2000) ("[A] bus passenger clearly expects that his bag may be handled. He does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner. But this is exactly what the agent did here. We therefore hold that the agent's physical manipu-

[various third parties' records] and a computerized summary located in a single clearinghouse of information.").⁴⁷

Third, the almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979. In *Smith*, the Supreme Court was actually considering whether local police could collect one person's phone records for calls made after the pen register was installed and for the limited purpose of a small-scale investigation of harassing phone calls. *See Smith*, 442 U.S. at 737, 99 S.Ct. 2577. The notion that the Government could collect similar data on hundreds of millions of people and retain that data for a five-year period, updating it with new data every day in perpetuity, was at best, in 1979, the stuff of science fiction. By comparison, the Government has at its disposal today the most advanced twenty-first century tools, allowing it to "store such records and efficiently mine them for information years into the future." *Jones*, 132 S.Ct. at 956 (Sotomayor, J., concurring). And these technologies are "cheap in comparison to conventional surveillance techniques and, by design, proceed[] surreptitiously," thereby "evad[ing] the ordinary checks that constrain abusive law enforcement practices: limited police . . . resources and community hostility." *Id.*⁴⁸

Finally, and most importantly, not only is the Government's ability to collect,

lation of petitioner's bag violated the Fourth Amendment.").

48. The unprecedented scope and technological sophistication of the NSA's program distinguish it not only from the *Smith* pen register, but also from metadata collections performed as part of routine criminal investigations. To be clear, this opinion is focusing only on the program before me and not any other law enforcement practices. Like the concurring justices in *Jones*, I cannot "identify with precision the point at which"

store, and analyze phone data greater now than it was in 1979, but the nature and quantity of the information contained in people's telephony metadata is much greater, as well. According to the 1979 U.S. Census, in that year, 71,958,000 homes had telephones available, while 6,614,000 did not. U.S. DEP'T OF COMMERCE & U.S. DEP'T OF HOUS. & URBAN DEV., ANNUAL HOUSING SURVEY: 1979, at 4 (1981) (Table A-1: Characteristics of the Housing Inventory: 1979 and 1970). In December 2012, there were a whopping 326,475,248 mobile subscriber connections in the United States, of which approximately 304 million were for phones and twenty-two million were for computers, tablets, and modems.⁴⁹ CTIA—The Wireless Ass'n ("CTIA"), *Wireless Industry Survey Results—December 1985 to December 2012*, at 2, 6 (2013) ("CTIA Survey Results");⁵⁰ see also Sixteenth Report, *In re Implementation of Section 6002(b) of Omnibus Budget Reconciliation Act*, WT Dkt. No. 11-186, at 9 (F.C.C. Mar. 21, 2013) ("[A]t the end of 2011 there were 298.3 million subscribers to mobile telephone, or voice, service, up nearly 4.6 percent from 285.1 million at the end of 2010."). The number of mobile subscribers in 2013 is more than 3,000 times greater than the 91,600 subscriber connections in 1984, IN-

bulk metadata collection becomes a search, but there is a substantial likelihood that the line was crossed under the circumstances presented in this case. See *Jones*, 132 S.Ct. at 964 (Alito, J., concurring).

49. The global total is 6.6 billion. ERICSSON, *Mobility Report on the Pulse of Networked Society*, at 4 (Nov.2013), available at <http://www.ericsson.com/res/docs/2013/ericsson-mobility-report-november-2013.pdf>.

50. http://files.ctia.org/pdf/CTIA_Survey_YE_2012_Graphics-FINAL.pdf.

51. Mobile phones are rapidly replacing traditional landlines, with 38.2% of households going "wireless-only" in 2012. CTIA, *Wire-*

DUS. ANALYSIS DIV., FED. COMM'CNS COMM'N, TRENDS IN TELEPHONE SERVICE 8 (1998), and more than triple the 97,035,925 subscribers in June 2000, CTI *Survey Results*, *supra*, at 4.⁵¹ It is now safe to assume that the vast majority of people reading this opinion have *at least* one cell phone within arm's reach (in addition to other mobile devices). Joanna Brenner, *Pew Internet: Mobile* (Sept. 18, 2013) (91% of American adults have a cell phone, 95–97% of adults age 18 to 49);⁵² CTIA, *Wireless Quick Facts* (last visited Dec. 10, 2013) ("CTIA *Quick Facts*") (wireless penetration—the number of active wireless units divided by total U.S. and territorial population—was 102.2%) as of December 2012).⁵³ In fact, some undoubtedly will be reading this opinion *on their cell-phones*. Maeve Duggan, *Cell Phone Activities 2013* (Sept. 19, 2013) (60% of cell phone owners use them to access internet).⁵⁴ Cell phones have also morphed into multi-purpose devices. They are now maps and music players. *Id.* (49% of cell phone owners use their phones to get directions and 48% to listen to music). They are cameras. Keith L. Alexander, *Camera phones become courthouse safety issue*, WASH. POST, Apr. 22, 2013, at B01. They are even lighters that people hold up at rock concerts. Andy Rathbun, *Cool 2 Know—Cellphone virtuosos*, NEWSDAY,

less Quick Facts, <http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts> (last visited Dec. 10, 2013); see also Jeffrey Sparshott, *More People Say Goodbye to Landlines*, WALL ST. J., Sept. 6, 2013, at A5.

52. <http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx>.

53. <http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts>.

54. <http://pewinternet.org/Reports/2013/Cell-Activities/Main-Findings.aspx>.

Apr. 20, 2005, at B02. They are ubiquitous as well. Count the phones at the bus stop, in a restaurant, or around the table at a work meeting or any given occasion. Thirty-four years ago, *none* of those phones would have been there.⁵⁵ Thirty-four years ago, city streets were lined with pay phones. Thirty-four years ago,

when people wanted to send “text messages,” they wrote letters and attached postage stamps.⁵⁶

Admittedly, what metadata *is* has not changed over time. As in *Smith*, the types of information at issue in this case are relatively limited: phone numbers dialed, date, time, and the like.⁵⁷ But the ubiquity

55. Mobile Telephone, BRITANNICA.COM, <http://www.britannica.com/EBchecked/topic/1482373/mobile-telephone?anchor=ref1079017> (last visited Dec. 13, 2013) (“[A] Japanese system was the first cellular system to be deployed, in 1979.”); Tom Farley, *Mobile telephone history*, TELEKTRONIKK, March/April 2005, at 28 (“An 88 cell system in the challenging cityscape of Tokyo began in December, 1979.... The first North American commercial system began in August, 1981 in Mexico City.”).

56. It is not clear from the pleadings whether “telephony metadata” and “comprehensive communications routing information” includes data relating to text messages. See *supra* note 16. If it does, then in 2012, the Government collected an additional *six billion* communications *each day* (69,635 *each second*). See Infographic—*Americans sent and received more than 69,000 texts every second in 2012*, CTIA.org (Nov. 25, 2013), <http://www.ctia.org/resource-library/facts-and-infographics/archive/americans-texts-2012-infographic>.

57. There are, however, a few noteworthy distinctions between the data at issue in *Smith* and the metadata that exists nowadays. For instance, the pen register in *Smith* did not tell the government whether calls were completed or the duration of any calls, *see Smith*, 442 U.S. at 741, 99 S.Ct. 2577, whereas that information is captured in the NSA’s metadata collection.

A much more significant difference is that telephony metadata can reveal the user’s location, *see generally New Jersey v. Earls*, 214 N.J. 564, 70 A.3d 630, 637–38 (2013), which in 1979 would have been entirely unnecessary given that landline phones are tethered to buildings. The most recent FISC order explicitly “does not authorize the production of cell site location information,” Oct. 11, 2013 Primary order at 3 n.1, and the Government has publicly disavowed such collection, *see Transcript of June 25, 2013 Newseum Special*

Program: NSA Surveillance Leaks: Facts and Fiction, Remarks of Robert Litt, Gen. Counsel, Office of Dir. of Nat’l Intelligence, *available at* <http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/887-transcript-newseum-special-program-nsa-surveillance-leaks-facts-and-fiction> (“I want to make perfectly clear we do not collect cellphone location information under this program, either GPS information or cell site tower information.”).

That said, not all FISC orders have been made public, and I have no idea how location data has been handled in the past. Plaintiffs do allege that location data has been collected, *see Second Am. Compl. ¶ 28; Pls.’ Mem. at 10–11*, and the Government’s brief does not refute that allegation (though one of its declarations does, *see Shea Decl. ¶ 15*). *See also supra* note 17. Moreover, the most recent FISC order states, and defendants concede, that “‘telephony metadata’ includes ... trunk identifier[s],” Oct. 11, 2013 Primary order at 3 n.1; Govt.’s Opp’n at 9, which apparently “can reveal where [each] call enter[s] the trunk system” and can be used to “locate a phone within approximately a square kilometer,” Patrick Di Justo, *What the N.S.A. Wants to Know About Your Calls*, NEW YORKER (June 7, 2013), <http://www.newyorker.com/online/blogs/elements/2013/06/what-the-nsa-wants-to-know-about-your-phone-calls.html>. And “if [the metadata] includes a request for every trunk identifier used throughout the interaction,” that “could allow a phone’s movements to be tracked.” *Id.* Recent news reports, though not confirmed by the Government, cause me to wonder whether the Government’s briefs are entirely forthcoming about the full scope of the Bulk Telephony Metadata Program. *See, e.g., Barton Gellman & Ashkan Soltani, NSA maps targets by their phones*, WASH. POST, Dec. 5, 2013, at A01.

The collection of location data would, of course, raise its own Fourth Amendment concerns, *see, e.g., In re Application of the United*

of phones has dramatically altered the *quantity* of information that is now available and, *more importantly*, what that information can tell the Government about people's lives. *See Quon*, 130 S.Ct. at 2630 ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy.... [And] the ubiquity of those devices has made them generally affordable"); *cf. Jones*, 132 S.Ct. at 956 (Sotomayor, J., concurring) (discussing the "substantial quantum of intimate information about any person" captured by GPS tracking). Put simply, people in 2013 have an entirely different relationship with phones than they did thirty-four years ago. As a result, people make calls and send text messages now that they would not (really, *could not*) have made or sent back when *Smith* was decided—for example, every phone call today between two people trying to locate one another in a public place. *See CTIA Quick Facts, supra* (2.3

States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3d Cir.2010) ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way.... [I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information."), but my decision on this preliminary injunction does *not* turn on whether the NSA has in fact collected that data as part of the bulk telephony metadata program.

58. The Government maintains that the metadata the NSA collects does not contain personal identifying information associated with each phone number, and in order to get that information the FBI must issue a national security letter ("NSL") to the phone company. Govt.'s Opp'n at 48–49; P.I. Hr'g Tr. at 44–45. Of course, NSLs do not require *any* judicial oversight, *see* 18 U.S.C. § 2709; 12 U.S.C. § 3414, 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 50 U.S.C. § 3162, meaning they are

trillion voice minutes used in 2012, up from 62.9 billion in 1997). This rapid and monumental shift towards a cell phone-centric culture means that the metadata from each person's phone "reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," *Jones*, 132 S.Ct. at 955 (Sotomayor, J., concurring), that could not have been gleaned from a data collection in 1979. *See also* Decl. of Prof. Edward W. Felten ("Felten Decl.") [Dkt. # 22-1], at ¶¶ 38–58. Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life. *See Maynard*, 615 F.3d at 562–63.⁵⁸ Whereas some may assume that these cultural changes will force people to "reconcile themselves" to an "inevitable" "diminution of privacy that new technology entails," *Jones*, 132 S.Ct. at 962 (Alito, J., concurring), I think it is more likely that these trends have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as reasonable.⁵⁹

hardly a check on potential abuses of the metadata collection. There is also nothing stopping the Government from skipping the NSL step altogether and using public databases or any of its other vast resources to match phone numbers with subscribers. *See, e.g.*, James Ball et al., *Covert surveillance: The reaction: 'They are tracking the calling patterns of the entire country'*, GUARDIAN, June 7, 2013, at 5 ("[W]hen cross-checked against other public records, the metadata can reveal someone's name, address, driver's licence, credit history, social security number and more."); Felten Decl. ¶ 19 & n.14; Suppl. Decl. of Prof. Edward W. Felten [Dkt. # 28], at ¶¶ 3–4 ("[I]t would be trivial for the government to obtain a subscriber's name once it has that subscriber's phone number.... It is extraordinarily easy to correlate a phone number with its unique owner.").

59. Public opinion polls bear this out. *See, e.g.*, Associated Press, *9/11 Anniversary: Poll finds public doubts growing on federal surveil-*

In sum, the *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones. Plaintiffs have alleged that they engage in conduct that exhibits a subjective expectation of privacy in the bulk, five-year historical record of their telephony metadata, *see Pls.’ Mem.* at 21; *Suppl. Klayman Aff.* ¶¶ 5, 10, 13; *Strange Aff.* ¶¶ 11, 19, and I have no reason to question the genuineness of those subjective beliefs.⁶⁰ The more difficult question, however, is whether their expectation of privacy is one that society is prepared to recognize as objectively reasonable and justifiable. As I said at the outset, the question before me is not whether *Smith* answers the question of whether people can have a reasonable expectation of privacy in telephony metadata under all circumstances. Rather, the question that I will ultimately have to answer when I reach the merits of this case someday is whether people have a reasonable

lance, privacy, Hous. CHRON., Sept. 11, 2013, at A6 (“Some 56 percent oppose the NSA’s collection of telephone records for future investigations even though they do not include actual conversations.”).

60. If plaintiffs lacked such a subjective expectation of privacy in all of their cell phone metadata, I would likely find that it is the result of “‘condition[ing]’ by influences alien to well-recognized Fourth Amendment freedoms.” *Smith*, 442 U.S. at 740 n.5, 99 S.Ct. 2577. In 1979, the Court announced that numbers dialed on a phone are not private, and since that time, the Government and courts have gradually (but significantly) expanded the scope of what that holding allows. Now, even local police departments are routinely requesting and obtaining massive cell phone “tower dumps,” each of which can capture data associated with thousands of innocent Americans’ phones. *See Ellen Nakashima, ‘Tower dumps’ give police masses of cellphone data*, WASH. POST, Dec. 9, 2013, at

able expectation of privacy that is violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to high-tech querying and analysis without any case-by-case judicial approval. For the many reasons set forth above, it is significantly likely that on that day, I will answer that question in plaintiffs’ favor.

ii. There Is a Significant Likelihood Plaintiffs Will Succeed in Showing that the Searches Are Unreasonable.

[23] Having found that a search occurred in this case, I next must “examin[e] the totality of the circumstances to determine whether [the] search is reasonable within the meaning of the Fourth Amendment.” *Samson v. California*, 547 U.S. 843, 848, 126 S.Ct. 2193, 165 L.Ed.2d 250 (2006) (internal quotation marks omitted). “[A]s a general matter, warrantless searches are *per se* unreasonable under the Fourth Amendment.” *Nat'l Fed'n of*

A01. Targeted tower dumps may be appropriate under certain circumstances and with appropriate oversight and limitations, *see In re Search of Cellular Tel. Towers*, 945 F.Supp.2d 769, 770–71, 2013 WL 1932881, at *2 (S.D.Tex. May 8, 2013) (requiring warrant and return of all irrelevant records to telecom provider for 77-tower dump of all data for five-minute period), and fortunately, that question is not before me here. The point is, however, that the experiences of many Americans—especially those who have grown up in the post-*Smith*, post-cell phone, post-PATRIOT Act age—might well be compared to those of the “refugee from a totalitarian country, unaware of this Nation’s traditions, [who] erroneously assume[] that police were continuously monitoring” telephony metadata. *Smith*, 442 U.S. at 740 n.5, 99 S.Ct. 2577. Accordingly, their “subjective expectations obviously could play no meaningful role in ascertaining . . . the scope of Fourth Amendment protection,” and “a normative inquiry would be proper.” *Id.*

Fed. Emps.–IAM v. Vilsack, 681 F.3d 483, 488–89 (D.C.Cir.2012) (quoting *Quon*, 130 S.Ct. at 2630); *see also Chandler v. Miller*, 520 U.S. 305, 313, 117 S.Ct. 1295, 137 L.Ed.2d 513 (1997) (“To be reasonable under the Fourth Amendment, a search ordinarily must be based on individualized suspicion of wrongdoing.”).

[24–27] The Supreme Court has recognized only a “few specifically established and well-delineated exceptions to that general rule,” *Nat'l Fed'n of Fed. Emps.–IAM*, 681 F.3d at 489 (quoting *Quon*, 130 S.Ct. at 2630), including one that applies when “special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable,” *id.* (quoting *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995)). “Even where the government claims ‘special needs,’ as it does in this case, ‘a warrantless search is generally unreasonable unless based on ‘some quantum of individualized suspicion.’” *Id.* (quoting *Skinner v. Ry. Labor Execs. Ass'n*, 489 U.S. 602, 624, 109 S.Ct. 1402, 103 L.Ed.2d 639 (1989)). Still, a suspicionless search may be reasonable “where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion.” *Id.* (quoting *Skinner*, 489 U.S. at 624, 109 S.Ct. 1402). As such, my task is to “balance the [plaintiffs’] privacy expectations against the government’s interests to determine whether it is impractical to require a warrant or some level of individual-

61. Suspicionless searches and seizures have also been allowed in other contexts not analyzed under the “special needs” framework, including administrative inspections of “closely regulated” businesses, *see New York v. Burger*, 482 U.S. 691, 107 S.Ct. 2636, 96 L.Ed.2d 601 (1987), searches of fire-damaged buildings for the purpose of determining the cause of the fire, *see Michigan v. Tyler*, 436

U.S. 499, 98 S.Ct. 1942, 56 L.Ed.2d 486 (1978), and highway checkpoints set up to catch intoxicated motorists and illegal entrants into the United States, *see Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 110 S.Ct. 2481, 110 L.Ed.2d 412 (1990); *United States v. Martinez-Fuerte*, 428 U.S. 543, 96 S.Ct. 3074, 49 L.Ed.2d 1116 (1976).

“Special needs” cases, not surprisingly, form something of a patchwork quilt. For example, schools and government employers are permitted under certain circumstances to test students and employees for drugs and alcohol, *see Earls*, 536 U.S. 822, 122 S.Ct. 2559, 153 L.Ed.2d 735; *Vernonia Sch. Dist.*, 515 U.S. 646, 115 S.Ct. 2386, 132 L.Ed.2d 564; *Von Raab*, 489 U.S. 656, 109 S.Ct. 1384, 103 L.Ed.2d 685; *Skinner*, 489 U.S. 602, 109 S.Ct. 1402, 103 L.Ed.2d 639, and officers may search probationers and parolees to ensure compliance with the rules of supervision, *see Griffin v. Wisconsin*, 483 U.S. 868, 107 S.Ct. 3164, 97 L.Ed.2d 709 (1987).⁶¹ The doctrine has also been applied in cases involving efforts to prevent acts of terrorism in crowded transportation centers. *See, e.g., Cassidy*

U.S. 499, 98 S.Ct. 1942, 56 L.Ed.2d 486 (1978), and highway checkpoints set up to catch intoxicated motorists and illegal entrants into the United States, *see Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 110 S.Ct. 2481, 110 L.Ed.2d 412 (1990); *United States v. Martinez-Fuerte*, 428 U.S. 543, 96 S.Ct. 3074, 49 L.Ed.2d 1116 (1976).

v. Chertoff, 471 F.3d 67 (2d Cir.2006) (upholding searches of carry-on bags and automobiles that passengers bring on ferries); MacWade v. Kelly, 460 F.3d 260 (2d Cir.2006) (upholding searches of bags in New York City subway system). To my knowledge, however, no court has ever recognized a special need sufficient to justify continuous, daily searches of virtually every American citizen without any particularized suspicion. In effect, the Government urges me to be the first non-FISC judge to sanction such a dragnet.

[28] For reasons I have already discussed at length, I find that plaintiffs have a very significant expectation of privacy in an aggregated collection of their telephony metadata covering the last five years, and the NSA's Bulk Telephony Metadata Program significantly intrudes on that expectation.⁶² Whether the program violates the Fourth Amendment will therefore turn

62. These privacy interests are not “mitigated . . . by the statutorily mandated restrictions on access to and dissemination of the metadata that are written into the FISC’s orders.” Govt.’s Opp’n at 51–52. First, there are no minimization procedures applicable at the collection stage; the Government acknowledges that FISC orders require the recipients to turn over all of their metadata without limit. See Oct. 11, 2013 Primary order at 3–4. Further, the most recent order of the FISC states that any trained NSA personnel can access the metadata, with “[t]echnical personnel” authorized to run queries even using non-RAS-approved selection terms for purposes of “perform[ing] those processes needed to make [the metadata] usable for intelligence analysis.” *Id.* at 5. The “[r]esults of any intelligence analysis queries,” meanwhile, “may be shared, *prior to minimization*, for intelligence analysis purposes among [trained] NSA analysts.” *Id.* at 12–13 (emphasis added); see also Shear Decl. ¶¶ 30, 32 (minimization procedures “guard against inappropriate or unauthorized *dissemination* of information relating to U.S. persons,” and “results of authorized queries of the metadata may be shared, *without minimization*, among trained NSA personnel for analysis purposes” (emphases added)). These procedures in no

on “the nature and immediacy of the government’s concerns and the efficacy of the [search] in meeting them.” *Earls*, 536 U.S. at 834, 122 S.Ct. 2559.

[29] The Government asserts that the Bulk Telephony Metadata Program serves the “programmatic purpose” of “identifying unknown terrorist operatives and preventing terrorist attacks.” Govt.’s Opp’n at 51—an interest that everyone, including this Court, agrees is “of the highest order of magnitude,” *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (FISA Ct. Rev.2008); see also *Haig v. Agee*, 453 U.S. 280, 307, 101 S.Ct. 2766, 69 L.Ed.2d 640 (1981) (“It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation.” (internal quotation marks omitted)).⁶³ A closer examination of the record, however, reveals that the Govern-

way mitigate the privacy intrusion that occurs when the NSA collects, queries, and analyzes metadata. And that’s even *assuming* the Government complies with all of its procedures—an assumption that is not supported by the NSA’s spotty track record to date. See *supra* notes 23–25 and accompanying text.

63. It bears noting that the Government’s interest in stopping and prosecuting terrorism has not led courts to abandon familiar doctrines that apply in criminal cases generally. See *United States v. Ressam*, 679 F.3d 1069, 1106 (9th Cir.2012) (Schroeder, J., dissenting) (collecting cases in which “courts have treated other issues in terrorism cases in ways that do not differ appreciably from more broadly applicable doctrines”). In fact, the Supreme Court once expressed in dicta that an otherwise impermissible roadblock “would almost certainly” be allowed “to thwart an imminent terrorist attack.” *City of Indianapolis v. Edmond*, 531 U.S. 32, 44, 121 S.Ct. 447, 148 L.Ed.2d 333 (2000) (emphases added). The Supreme Court has never suggested that all Fourth Amendment protections must defer to any Government action that purportedly serves national security or counterterrorism interests.

ment's interest is a bit more nuanced—it is not merely to investigate potential terrorists, but rather, to do so *faster* than other investigative methods might allow. Indeed, the affidavits in support of the Government's brief repeatedly emphasize this interest in speed. For example, according to SID Director Shea, the primary advantage of the bulk metadata collection is that "it enables the Government to *quickly* analyze past connections and chains of communication," and "increases the NSA's ability to *rapidly* detect persons affiliated with the identified foreign terrorist organizations." Shea Decl. ¶ 46 (emphases added); *see also id.* ¶ 59 ("Any other means that might be used to attempt to conduct similar analyses would require *multiple, time-consuming steps* that would frustrate needed *rapid* analysis in emergent situations, and could fail to capture some data available through bulk metadata analysis.") (emphases added)). FBI Acting Assistant Director of the Counterterrorism Division Robert J. Holley echoes Director Shea's emphasis on speed: "It is imperative that the United States Government have the capability to *rapidly* identify any terrorist threat inside the United States." Holley Decl. ¶ 4 (emphasis added); *see also id.* ¶¶ 28–29 ("[T]he *agility* of querying the metadata collected by NSA under this program allows for more *immediate* contact chaining, which is significant in *time-sensitive* situations.... The *delay* inherent in issuing new national security letters would necessarily mean losing *valuable time*.... [A]gggregating the NSA telephony metadata from different telecommunications providers enhances and *expedites* the ability to identify chains of communications across multiple providers.") (emphases added)).

Yet, turning to the efficacy prong, the Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an immin-

ent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature. In fact, none of the three "recent episodes" cited by the Government that supposedly "illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack" involved any apparent urgency. *See* Holley Decl. ¶¶ 24–26. In the first example, the FBI learned of a terrorist plot still "in its early stages" and investigated that plot before turning to the metadata "to ensure that all potential connections were identified." *Id.* ¶ 24. Assistant Director Holley does not say that the metadata revealed any new information—much less time-sensitive information—that had not already come to light in the investigation up to that point. *Id.* In the second example, it appears that the metadata analysis was used only after the terrorist was arrested "to establish [his] foreign ties and put them in context with his U.S. based planning efforts." *Id.* ¶ 25. And in the third, the metadata analysis "revealed a previously unknown number for [a] co-conspirator ... and corroborated his connection to [the target of the investigation] as well as to other U.S.-based extremists." *Id.* ¶ 26. Again, there is no indication that these revelations were immediately useful or that they prevented an impending attack. Assistant Director Holley even concedes that bulk metadata analysis only "*sometimes* provides information earlier than the FBI's other investigative methods and techniques." *Id.* ¶ 23 (emphasis added).⁶⁴ Given the limited record before me at this point in the litigation—most notably, the utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics—I have serious doubts about the efficacy of the metadata collection program

⁶⁴. Such candor is as refreshing as it is rare.

as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism.⁶⁵ See *Chandler*, 520 U.S. at 318–19, 117 S.Ct. 1295 (“Notably lacking in respondents’ presentation is any indication of a concrete danger demanding departure from the Fourth Amendment’s main rule.”). Thus, plaintiffs have a substantial likelihood of showing that their privacy interests outweigh the Government’s interest in collecting and analyzing bulk telephony metadata and therefore the NSA’s bulk collection program is indeed an unreasonable search under the Fourth Amendment.⁶⁶

[30–32] I realize, of course, that such a holding might appear to conflict with other trial courts, see, e.g., *United States v. Moalin*, Crim. No. 10–4246, 2013 WL 6079518, at *5–8 (S.D.Cal. Nov. 18, 2013) (holding that bulk telephony metadata collection does not violate Fourth Amendment); *United States v. Graham*, 846 F.Supp.2d 384, 390–405 (D.Md.2012) (holding that defendants had no reasonable expectation of privacy in historical cell-site location information); *United States v. Gordon*, Crim.

No. 09–153–02, 2012 WL 8499876, at *1–2 (D.D.C. Feb. 6, 2012) (same), and with longstanding doctrine that courts have applied in other contexts, see, e.g., *Smith*, 442 U.S. at 741–46, 99 S.Ct. 2577, *Miller*, 425 U.S. at 443, 96 S.Ct. 1619. Nevertheless, in reaching this decision, I find comfort in the statement in the Supreme Court’s recent majority opinion in *Jones* that “[a]t bottom, we must ‘assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’” 132 S.Ct. at 950 (2012) (quoting *Kyllo*, 533 U.S. at 34, 121 S.Ct. 2038). Indeed, as the Supreme Court noted more than a decade before *Smith*, “[t]he basic purpose of th[e Fourth] Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.” *Camara v. Mun. Court*, 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967) (emphasis added); see also *Quon*, 130 S.Ct. at 2627 (“The Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government,

65. The Government could have requested permission to present additional, potentially classified evidence *in camera*, but it chose not to do so. Although the Government has publicly asserted that the NSA’s surveillance programs have prevented fifty-four terrorist attacks, no proof of that has been put before me. See also Justin Elliott & Theodoric Meyer, *Claim on ‘Attacks Thwarted’ by NSA Spreads Despite Lack of Evidence*, PROPUBLICA.ORG (Oct. 23, 2013), <http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence> (“‘We’ve heard over and over again the assertion that 54 terrorist plots were thwarted’ by the [NSA’s] programs.... ‘That’s plainly wrong.... These weren’t all plots and they weren’t all thwarted. The American people are getting left with the inaccurate impression of the effectiveness of the NSA programs.’” (quoting Sen. Patrick Leahy)); Ellen Nakashima, *NSA’s need to keep database questioned*, WASH. POST, Aug. 9, 2013, at A01 (“[Senator Ron] Wyden noted that

[two suspects arrested after an investigation that involved use of the NSA’s metadata database] were arrested ‘months or years after they were first identified’ by mining the phone logs.”).

66. The Government points out that it could obtain plaintiffs’ metadata through other means that potentially raise fewer Fourth Amendment concerns. See Govt.’s Opp’n at 6 (“The records must be of a type obtainable by either a grand jury subpoena, or an order issued by a U.S. court directing the production of records or tangible things.” (citing 50 U.S.C. § 1861(c)(2)(D)); Holley Decl. ¶ 14 (“In theory, the FBI could seek a new set of orders on a daily basis for the records created within the preceding 24 hours.”)). Even if true, “[t]he fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment.” *Kyllo*, 533 U.S. at 35 n.2, 121 S.Ct. 2038.

without regard to whether the government actor is investigating crime or performing another function.” (internal quotation marks omitted)). The Fourth Amendment typically requires “a neutral and detached authority be interposed between the police and the public,” and it is offended by “general warrants” and laws that allow searches to be conducted “indiscriminately and without regard to their connection with [a] crime under investigation.” *Berger v. New York*, 388 U.S. 41, 54, 59, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967). I cannot imagine a more “indiscriminate” and “arbitrary invasion” than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval. Surely, such a program infringes on “that degree of privacy” that the Founders enshrined in the Fourth Amendment. Indeed, I have little doubt that the author of our Constitution, James Madison, who cautioned us to beware “the abridgement of freedom of the people by gradual and silent encroachments by those in power,” would be aghast.⁶⁷

2. Plaintiffs Will Suffer Irreparable Harm Absent Injunctive Relief.

[33, 34] “It has long been established that the loss of constitutional freedoms, ‘for even minimal periods of time, unquestionably constitutes irreparable injury.’” *Mills v. District of Columbia*, 571 F.3d 1304, 1312 (D.C.Cir.2009) (quoting *Elrod v. Burns*, 427 U.S. 347, 373, 96 S.Ct. 2673, 49 L.Ed.2d 547 (1976) (plurality opinion)). As in this case, the court in *Mills* was confronted with an alleged Fourth Amendment violation: a “Neighborhood Safety

67. James Madison, Speech in the Virginia Ratifying Convention on Control of the Military (June 16, 1788), in THE HISTORY OF THE VIRGINIA FEDERAL CONVENTION OF 1788, WITH SOME ACCOUNT OF EMINENT VIRGINIANS OF THAT ERA WHO WERE MEMBERS OF THE BODY (Vol.1) 130

Zones” traffic checkpoint for vehicles entering a high-crime neighborhood in Washington, DC. *Id.* at 1306. After finding a strong likelihood of success on the merits, our Circuit Court had little to say on the irreparable injury prong, instead relying on the statement at the beginning of this paragraph that a constitutional violation, even of minimal duration, constitutes irreparable injury. Plaintiffs in this case have also shown a strong likelihood of success on the merits of a Fourth Amendment claim. As such, they too have adequately demonstrated irreparable injury.

3. The Public Interest and Potential Injury to Other Interested Parties Also Weigh in Favor of Injunctive Relief.

[35, 36] “[I]t is always in the public interest to prevent the violation of a party’s constitutional rights.” *Am. Freedom Def. Initiative v. Wash. Metro. Area Transit Auth.*, 898 F.Supp.2d 73, 84 (D.D.C. 2012) (quoting *G & V Lounge, Inc. v. Mich. Liquor Control Comm’n*, 23 F.3d 1071, 1079 (6th Cir.1994); *see also Hobby Lobby Stores, Inc. v. Sebelius*, 723 F.3d 1114, 1145 (10th Cir.2013) (same), cert. granted, — U.S. —, 134 S.Ct. 678, 187 L.Ed.2d 544, 2013 WL 5297798 (2013); *Melendres v. Arpaio*, 695 F.3d 990, 1002 (9th Cir.2012) (same); *Nat'l Fed'n of Fed. Emps. v. Carlucci*, 680 F.Supp. 416 (D.D.C.1988) (“[T]he public interest lies in enjoining unconstitutional searches.”). That interest looms large in this case, given the significant privacy interests at stake and the unprecedented scope of the NSA’s collection and querying efforts, which likely violate the Fourth Amendment. Thus,

(Hugh Blair Grigsby et al. eds., 1890) (“Since the general civilization of mankind, I believe there are more instances of the abridgement of freedom of the people by gradual and silent encroachments by those in power than by violent and sudden usurpations.”).

the public interest weighs heavily in favor of granting an injunction.

The Government responds that the public's interest in combating terrorism is of paramount importance, *see Govt.'s Opp'n at 64–65*—a proposition that I accept without question. But the Government offers no real explanation as to how granting relief to these plaintiffs would be detrimental to that interest. Instead, the Government says that it will be burdensome to comply with any order that requires the NSA to remove plaintiffs from its database. *See id.* at 65; Shea Decl. ¶ 65. Of course, the public has no interest in saving the Government from the burdens of complying with the Constitution! Then, the Government frets that such an order “could ultimately have a degrading effect on the utility of the program if an injunction in this case precipitated successful requests for such relief by other litigants.” Govt.'s Opp'n at 65 (citing Shea Decl. ¶ 65). For reasons already explained, I am not convinced at this point in the litigation that the NSA's database has ever truly served the purpose of rapidly identifying terrorists in time-sensitive investigations, and so I am *certainly* not convinced that the removal of two individuals from the database will “degrade” the program in any meaningful sense.⁶⁸ I will leave it to other judges to decide how to handle any future litigation in their courts.

68. To the extent that removing plaintiffs from the database would create a risk of “eliminating, or cutting off potential call chains,” Shea Decl. ¶ 65, the Government concedes that the odds of this happening are minuscule. *See Govt.'s Opp'n at 2 (“[O]nly a tiny fraction of the collected metadata is ever reviewed....”); Shea Decl. ¶ 23 (“Only the tiny fraction of the telephony metadata records that are responsive to queries authorized under the RAS standard are extracted, reviewed, or disseminated....”).*

69. For reasons stated at the outset, this relief is limited to *Klayman I* plaintiffs Larry Klay-

CONCLUSION

This case is yet the latest chapter in the Judiciary's continuing challenge to balance the national security interests of the United States with the individual liberties of our citizens. The Government, in its understandable zeal to protect our homeland, has crafted a counterterrorism program with respect to telephone metadata that strikes the balance based in large part on a thirty-four year old Supreme Court precedent, the relevance of which has been eclipsed by technological advances and a cell phone-centric lifestyle heretofore inconceivable. In the months ahead, other Article III courts, no doubt, will wrestle to find the proper balance consistent with our constitutional system. But in the meantime, for all the above reasons, I will grant Larry Klayman's and Charles Strange's requests for an injunction⁶⁹ and enter an order that (1) bars the Government from collecting, as part of the NSA's Bulk Telephony Metadata Program, any telephony metadata associated with their personal Verizon accounts and (2) requires the Government to destroy any such metadata in its possession that was collected through the bulk collection program.⁷⁰

[37] However, in light of the significant national security interests at stake in this case and the novelty of the constitutional issues, I will stay my order pending ap-

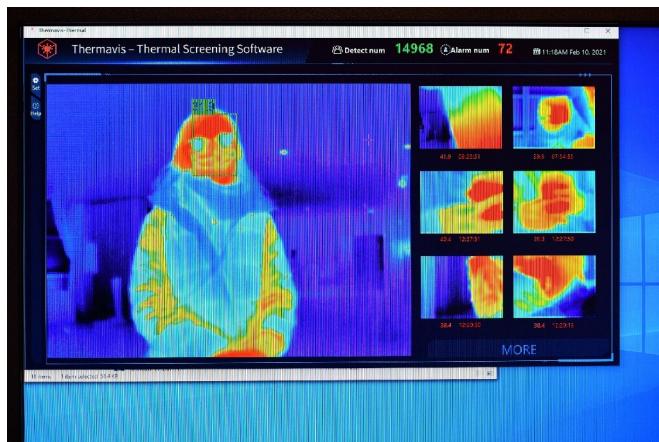
man and Charles Strange. I will deny Mary Ann Strange's motion and the motion in *Klayman II*.

70. Although it is true that granting plaintiffs the relief they request will force the Government to identify plaintiffs' phone numbers and metadata records, and then subject them to otherwise unnecessary individual scrutiny, *see Shea Decl. ¶ 64*, that is the only way to remedy the constitutional violations that plaintiffs are substantially likely to prove on the merits.

peal.⁷¹ In doing so, I hereby give the Government fair notice that should my ruling be upheld, this order will go into effect forthwith. Accordingly, I fully expect that during the appellate process, which will consume at least the next six months, the Government will take whatever steps necessary to prepare itself to comply with this order when, and if, it is upheld. Suffice it to say, requesting further time to comply with this order months from now will not be well received and could result in collateral sanctions.

Privacy faces risks in tech-infused post-COVID workplace

21 February 2021, by Rob Lever



A thermal imaging camera are displayed on a screen as a person waits at the reception desk at the St Giles Hotel near Heathrow Airport in west London, in an example of technology being used to screen for Covid-19 symptoms

People returning to work following the long pandemic will find an array of tech-infused gadgetry to improve workplace safety but which could pose risks for long-term personal and medical privacy.

Temperature checks, distance monitors, digital "passports," wellness surveys and robotic cleaning and disinfection systems are being deployed in many workplaces seeking to reopen.

Tech giants and startups are offering solutions which include computer vision detection of vital signs to wearables which can offer early indications of the onset of COVID-19 and apps that keep track of [health](#) metrics.

Salesforce and IBM have partnered on a "digital health pass" to let people share their vaccination and [health status](#) on their smartphone.

Clear, a tech startup known for airport screening,

has created its own health pass which is being used by organizations such as the National Hockey League and MGM Resorts.

Fitbit, the wearable tech maker recently acquired by Google, has its own "Ready for Work" program that includes daily check-ins using data from its devices.

Fitbit is equipping some 1,000 NASA employees with wearables as part of a pilot program which requires a daily log-in using various health metrics which will be tracked by the space agency.

Microsoft and insurance giant United HealthCare have deployed a ProtectWell app which includes a daily symptom screener, and Amazon has deployed a "distance assistant" in its warehouses to help employees maintain safe distances.

And a large coalition of technology firms and health organizations are working on a digital vaccination certificate, which can be used on smartphones to show evidence of inoculation for COVID-19.



A member of staff at the University of Bolton in northern England has his body temperature checked by an automatic walk-through scanner to help to mitigate the spread of the novel coronavirus

'Blurs the lines'

With these systems, employees may face screenings even as they enter a building lobby, and monitoring in elevators, hallways and throughout the workplace.

The monitoring "blurs the line between people's workplace and personal lives," said Darrell West, a Brookings Institution vice president with the think tank's Center for Technology Innovation.

"It erodes longstanding medical privacy protections for many different workers."

A report last year by the consumer activist group Public Citizen identified at least 50 apps and technologies released during the pandemic "marketed as workplace surveillance tools to combat COVID-19."

The report said some systems go so far as identifying people who may not spend enough time in front of a sink to note inadequate hand-washing.

"The invasion of privacy that workers face is alarming, especially considering that the effectiveness of these technologies in mitigating the spread of COVID-19 has not yet been established," the report said.

The group said there should be clear rules on collection and storage of data, with better disclosure to employees.

A delicate balance

Employers face a delicate balance as they try to ensure [workplace safety](#) without intruding on privacy, said Forrest Briscoe, professor of management and organization at Penn State University.



This personal programmable robot from Misty Robotics may be used companies to help in health screening to limit the spread of Covid-19

Briscoe said there are legitimate reasons and precedents for requiring proof of vaccination. But these sometimes conflict with medical privacy regulations which limit a company's access to employee health data.

"You don't want the employer accessing that information for work-related decisions," Briscoe said.

Briscoe said many employers are relying on third-party tech vendors to handle the monitoring, but that has its risks as well.

"Using third-party vendors will keep the data separate," he said.

"But for some companies their business model involves gathering data and using it for some monetizable purpose and that poses a risk to privacy."

The global health crisis has inspired startups around the world to seek innovative ways to limit virus transmission, with some of those products shown at the 2021 Consumer Electronics Show.

Taiwan-based FaceHeart demonstrated software which can be installed in cameras for contactless measurement of vital signs to screen for shortness

of breath, [high fever](#), dehydration, elevated heart rate and other symptoms which are early indicators of COVID-19.

Drone maker Draganfly showcased camera technology which can be used to offer alerts on social distancing, and also detect changes in people's vital signs which may be early indicators of COVID-19 infection.

A programmable robot from Misty Robotics, also shown at CES, can be adapted as a health check monitor and can also be designed to disinfect frequently used surfaces like door handles, according to the company.

But there are risks in relying too much on technologies which may be unproven or inaccurate, such as trying to detect fevers with thermal cameras among moving people, said Jay Stanley, a privacy researcher and analyst with the American Civil Liberties Union.

"Employers have a legitimate interest in safeguarding workplaces and keeping employees healthy in the context of the pandemic," Stanley said.

"But what I would worry about is employers using the pandemic to pluck and store information in a systematic way beyond what is necessary to protect health."

© 2021 AFP

APA citation: Privacy faces risks in tech-infused post-COVID workplace (2021, February 21) retrieved 21 February 2021 from

<https://techxplore.com/news/2021-02-privacy-tech-infused-post-covid-workplace.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.

We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.

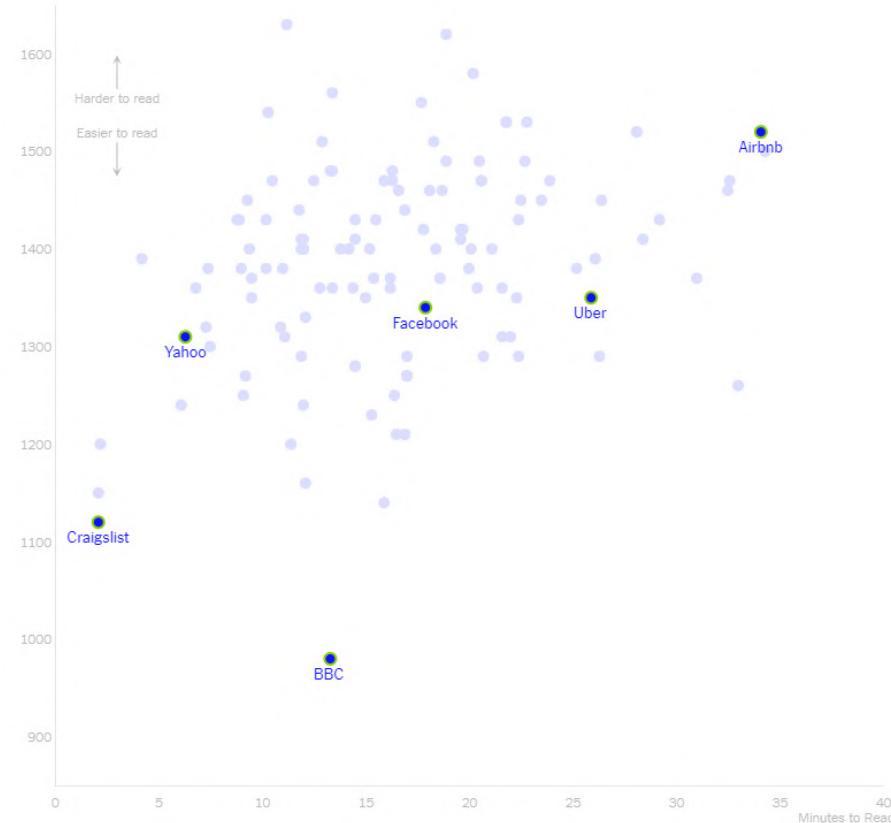
By Kevin Litman-Navarro

In the background here are several privacy policies from major tech and media platforms. Like most privacy policies, they're verbose and full of legal jargon — and opaquely establish companies' justifications for collecting and selling your data. The data market has become the engine of the internet, and these privacy policies we agree to but don't fully understand help fuel it.

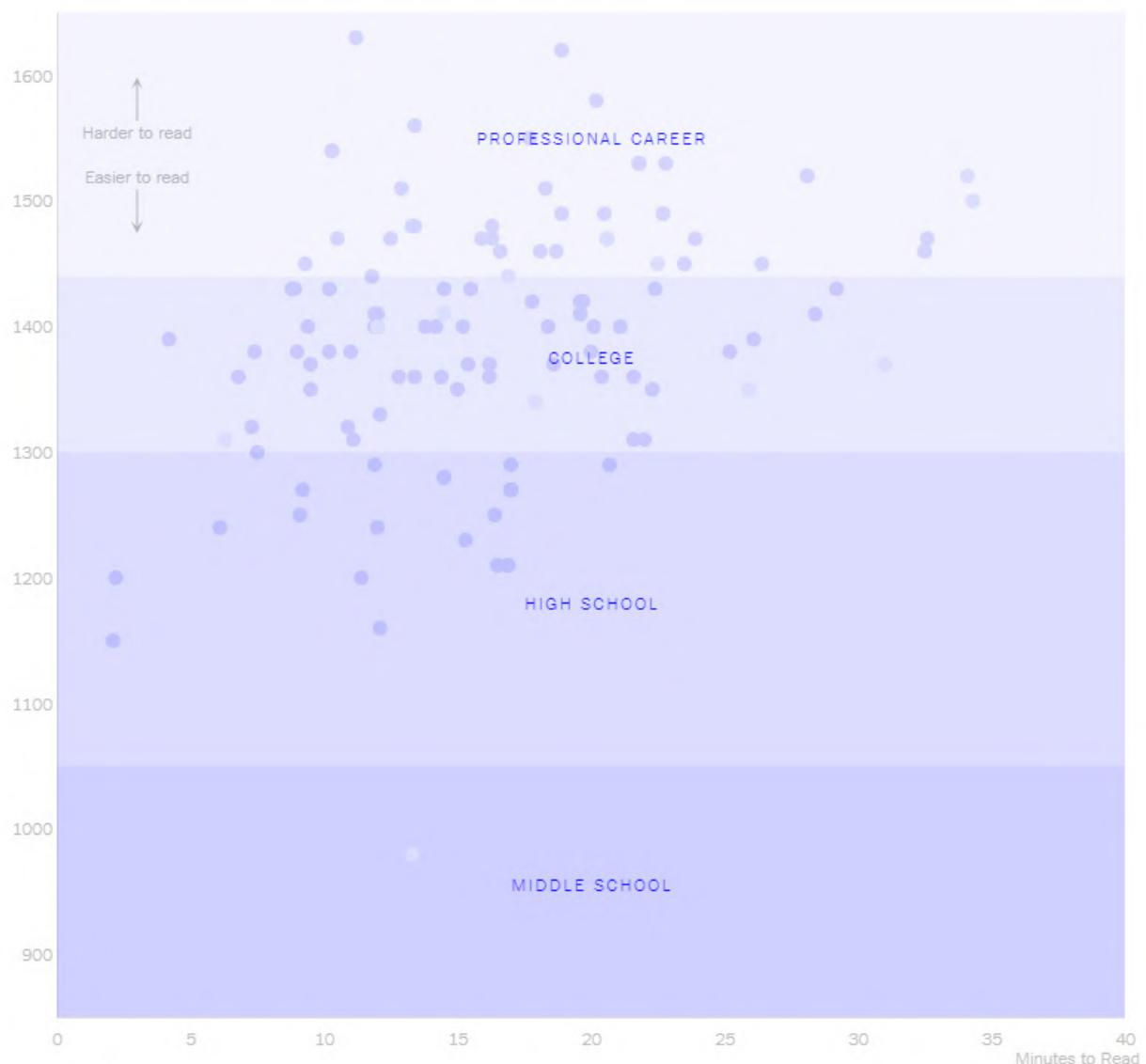
To see exactly how inscrutable they have become, I analyzed the length and readability of privacy policies from nearly 150 popular websites and apps. Facebook's privacy policy, for example, takes around 18 minutes to read in its entirety — slightly above average for the policies I tested.



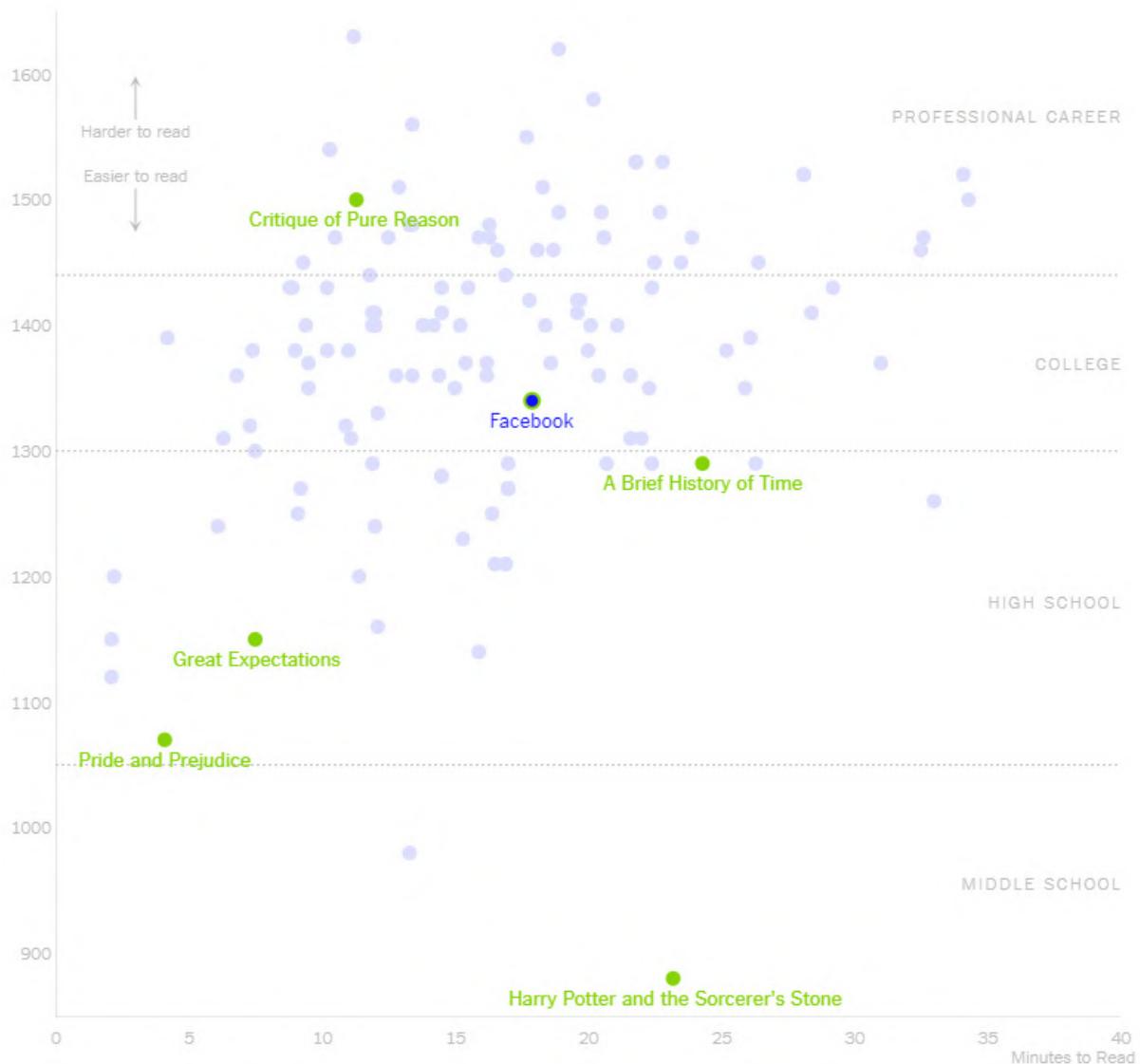
Then I tested how easy it was to understand each policy using the Lexile test developed by the education company Metametrics. The test measures a text's complexity based on factors like sentence length and the difficulty of vocabulary.



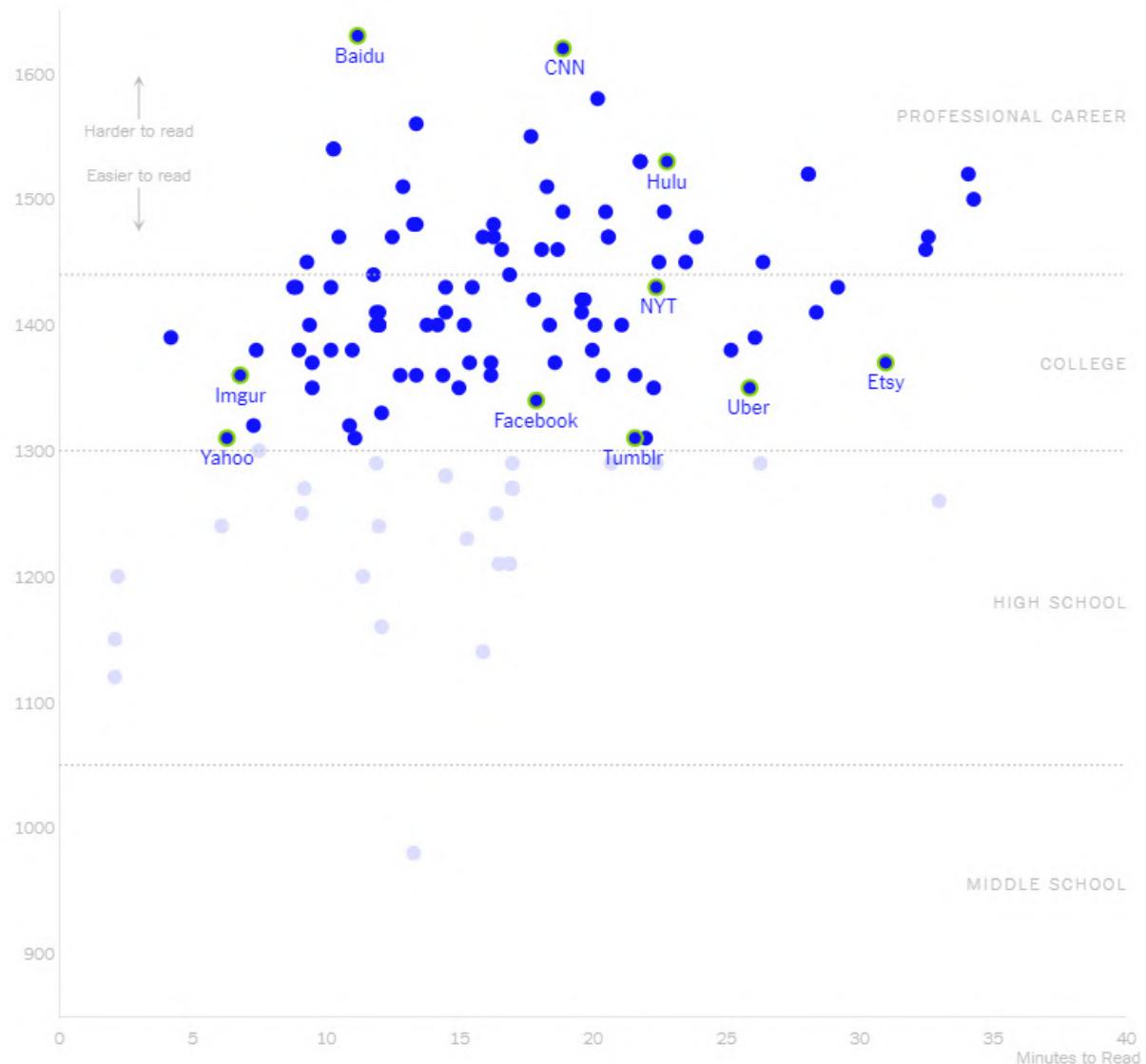
To be successful in college, people need to understand texts with a score of 1300. People in the professions, like doctors and lawyers, should be able to understand materials with scores of 1440, while ninth graders should understand texts that score above 1050 to be on track for college or a career by the time they graduate. Many privacy policies exceed these standards.



For comparison, here are the scores for some classic texts. Only Immanuel Kant's famously difficult "Critique of Pure Reason" registers a more challenging readability score than Facebook's privacy policy. (To calculate their reading time, I measured the first chapter of each text.)



The vast majority of these privacy policies exceed the college reading level. And according to the most recent literacy survey conducted by the National Center for Education Statistics, over half of Americans may struggle to comprehend dense, lengthy texts. That means a significant chunk of the data collection economy is based on consenting to complicated documents that many Americans can't understand.



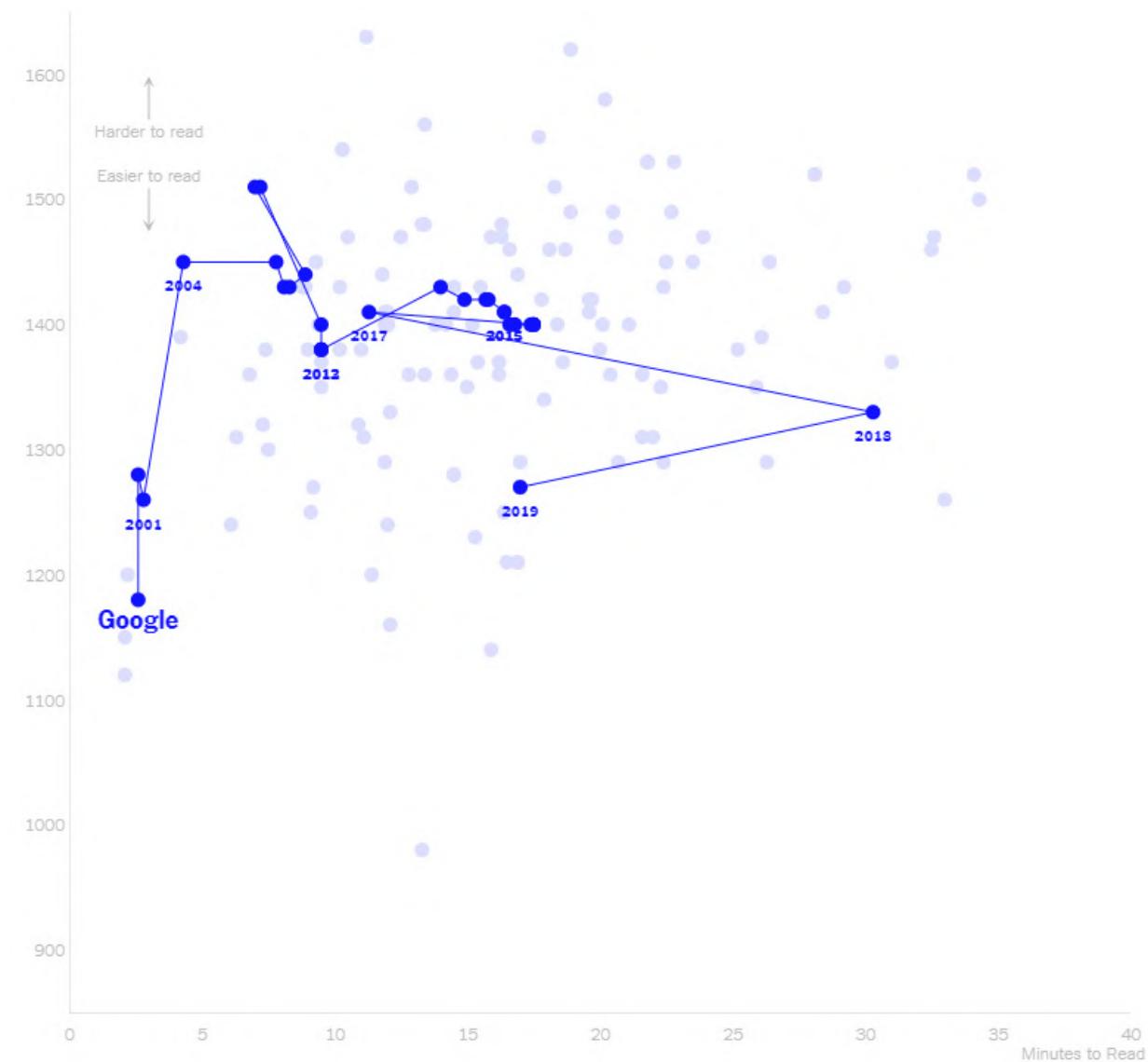
The BBC has an unusually readable privacy policy. It's written in short, declarative sentences, using plain language. Here's how the policy outlines the BBC's guidelines for collecting and using personal data:

"We have to have a valid reason to use your personal information. It's called the 'lawful basis for processing.' Sometimes we might ask your permission to do things, like when you subscribe to an email. Other times, when you'd reasonably expect us to use your personal information, we don't ask your permission, but only when: the law says it's fine to use it, and it fits with the rights you have."

Airbnb's privacy policy, on the other hand, is particularly inscrutable. It's full of long, jargon-laden sentences that obscure Airbnb's data practices and provides cover to use data in expansive ways. For example, here is how Airbnb justifies collecting users' personal information. Vague language like "adequate performance" and "legitimate interest" allows for a wide range of interpretation, providing flexibility for Airbnb to defend its data practices in a lawsuit while making it harder for users to understand what is being done with their data.

"This information is necessary for the adequate performance of the contract between you and us and to allow us to comply with our legal obligations."

Things weren't always this bad. Google's privacy policy evolved over two decades — along with its increasingly complicated data collection practices — from a two-minute read in 1999 to a peak of 30 minutes by 2018.



The policy became more readable at the expense of brevity after the introduction of the General Data Protection Regulation, the European Union data privacy protection framework that went into effect a year ago. The regulation includes a clause requiring privacy policies to be delivered in a “concise, transparent and intelligible form, using clear and plain language.”

In the most recent update of its policy, Google chopped off a glossary of technical terms to make it more readable and concise.

Despite efforts like the General Data Protection Regulation to make policies more accessible, there seems to be an intractable tradeoff between a policy’s readability and length. Even policies that are shorter and easier to read can be impenetrable, given the amount of background knowledge required to understand how things like cookies and IP addresses play a role in data collection.

“You’re confused into thinking these are there to inform users, as opposed to protect companies,” said Albert Gidari, the consulting director of privacy at the Stanford Center for Internet and Society.

As data collection practices become more sophisticated (and invasive), it’s unlikely that privacy policies will become any easier to comprehend. And if states continue to draft their own data protection laws, as California is doing with its Consumer Privacy Act, privacy policies could balloon with location-specific addendums.

[If you use technology, someone is using your information. We’ll tell you how — and what you can do about it. [Sign up for our limited-run newsletter.](#)]

According to Jen King, the director of consumer privacy at the Center for Internet and Society, this doesn’t mean we should throw out privacy policies entirely — we just need a fresh start.

“These are documents created by lawyers, for lawyers. They were never created as a consumer tool,” Dr. King said. “What would we do if we actually started over and did this from a human-centric point of view, knowing what we know now about how humans process information online?”

So what might a useful privacy policy look like?

Consumers don’t need a technical understanding of data collection processes in order to protect their personal information. Instead of explaining the excruciatingly complicated inner workings of the data marketplace, privacy policies should help people decide how they want to present themselves online. We tend to go on the internet privately — on our phones or at home — which gives the impression that our activities are also private. But, often, we’re more visible than ever.

A good privacy policy would help users understand how exposed they are: Something as simple as a list of companies that might purchase and use your personal information could go a long way towards setting a new bar for privacy-conscious behavior. For example, if you know that your weather app is constantly tracking your whereabouts and selling your location data as marketing research, you might want to turn off your location services entirely, or find a new app.

Until we reshape privacy policies to meet our needs — or we find a suitable replacement — it's probably best to act with one rule in mind. To be clear and concise: Someone's always watching.

Kevin Litman-Navarro is a writer and data journalist.

Like other media companies, The Times collects data on its visitors when they read stories like this one. For more detail please see our privacy policy and our publisher's description of The Times's practices and continued steps to increase transparency and protections.

Follow @privacyproject on Twitter and The New York Times Opinion Section on Facebook and Instagram.

Summary: The Supreme Court Rules in *Carpenter v. United States*

By **Sabrina McCubbin** Friday, June 22, 2018, 2:05 PM

Privacy Paradox: Rethinking Solitude

On Friday, June 22, the Supreme Court issued its much-anticipated opinion in *Carpenter v. United States*, holding that a warrant is required for police to access cell site location information from a cell phone company—the detailed geolocation information generated by a cellphone’s communication with cell towers. As predicted, Chief Justice Roberts authored the majority opinion, reversing the Sixth Circuit’s decision. He was joined by Justices Ginsburg, Breyer, Sotomayor and Kagan. The remaining four justices, Justices Kennedy, Thomas, Alito, and Gorsuch each filed separate dissenting opinions.

Background

Legal Background

The Stored Communications Act (SCA), part of the Electronic Communications Privacy Act (ECPA), creates privacy protections for the content of stored communications and the related non-content information. Orders made under Section 2703(d), known as 2703(d) orders, can compel the production of the content of stored communications or related non-content information, when “specific and articulable facts show[] that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” This standard of suspicion is considerably lower than the probable cause required for a typical warrant.

Also relevant to this decision are three earlier Supreme Court decisions: *United States v. Miller*, which addressed police access to business records held by third parties; *Smith v. Maryland*, which addressed police access to non-content phone records; and *United States v. Jones*, which dealt with police use of a geolocation device.

In *United States v. Miller*, the Court held that a defendant had no right to privacy in his banking records, as they were business records belonging to the bank. In *Smith v. Maryland*, the Court held that police did not require a warrant to use a pen register to monitor a suspect’s outgoing call data. *United States v. Miller* and *Smith v. Maryland* are examples of the application of the third-party doctrine—the legal principle that when an individual voluntarily gives information to a third party, the privacy interest in that information is forfeit. Because *Carpenter* involved records acquired from cell phone companies, the third-party doctrine was critical to the government’s arguments.

In *United States v. Jones*, the court addressed whether police use of a GPS tracking device required a warrant. Although Justice Scalia’s majority opinion focused on the police placement of the device as a trespass, Justices Alito and Sotomayor each focused their concurrence on the idea that monitoring an individual’s location over time is an invasion of privacy on its own. The idea that the aggregation of data over time can create a much more detailed and privacy-invasive picture is referred to as “mosaic theory.” These concurrences were cited frequently in the decision, and, as Orin Kerr described, played a key role in Carpenter’s brief.

Technical Background

At issue in this case was whether cell-site location information (CSLI), could be accessed by law enforcement without a warrant. CSLI is generated when a phone communicates with a cell tower. Sometimes this data is generated by a user’s *intentional* actions—by placing a phone call, sending a text message, or turning the phone on, the user causes the phone to communicate with the nearest cell tower. CSLI can also be generated *automatically*—when a phone receives a text message, or when the phone sends a periodic update to the network, for example. The greater the concentration of cell towers, the more accurate the location data will be. This means that it is easier to pin down an individual’s precise location in an urban area than in a rural one. Cell phone companies keep records of CSLI for business purposes, but this information can be used to reconstruct the movements of a particular phone over a long period of time.

Factual Background

In April 2011, four men were arrested in connection with a string of armed robberies of Radio Shack and T-Mobile stores. One of these men confessed that the group was responsible for the robberies, and that as many as 15 other men had participated in the crimes as getaway drivers and lookouts. He gave the FBI his personal cell phone number and the phone numbers of the others involved. The FBI then used the man’s call logs to identify additional phone numbers he had contacted around the time of the robberies.

The FBI then applied for 2703(d) orders to produce the “transactional records” from 16 phone numbers, including Carpenter’s. The transactional records requested included subscriber information, toll records, call detail records, and numbers dialed, as well as “cell site information for the target telephones at call origination and at call termination for incoming and outgoing calls.” Three magistrate judges found that the FBI had met the standards of suspicion required by the SCA, and issued the requested 2703(d) orders.

Procedural History

Two of the conspirators, Timothy Carpenter and Timothy Sanders, were eventually charged with aiding and abetting robbery affecting interstate commerce and the use or carriage of a firearm in violation of the Hobbs Act. At trial, the FBI explained that the CSLI acquired through 2703(d) orders had placed the two men’s phone within a half-mile to two miles of each robbery. Carpenter and Sanders sought to suppress the CSLI evidence under the Fourth Amendment, but the district court denied the motion. Both men were convicted, and both appealed.

On appeal to the Sixth Circuit, Carpenter challenged the district court’s denial of his motion to suppress the CSLI. Carpenter argued that the acquisition of CSLI through a 2703(d) order was unconstitutional, because it was a search within the meaning of the Fourth Amendment, and should have only been accessible with a warrant based on probable cause. The Sixth Circuit rejected Carpenter’s arguments, relying on *Smith v. Maryland* to hold that the data were business records, not protected by the Fourth Amendment.

On June 5, 2017, the Supreme Court granted certiorari. A wide range of amici filed briefs in this case, from Orin Kerr, who wrote in support of the government, to several privacy advocacy organizations who wrote in support of Carpenter. Oral arguments were held on Nov. 29, 2017.

Majority Opinion

Chief Justice Roberts’ majority opinion begins with a quick lesson on the history of the Fourth Amendment. Quoting the Supreme Court’s ruling in *Camara v. Municipal Court of City and County of San Francisco*, he notes that the court has recognized that the amendment’s purpose “is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.” He describes the evolution of Fourth Amendment doctrine from its early days of relating closely to common-law trespass to the development of the “reasonable expectation of privacy” doctrine under *Katz v. United States*, which established the modern understanding that the Fourth Amendment “protects people, not places.”

Roberts also notes that the development of technology has required the court to find ways to preserve privacy from the government even when surveillance tools have enhanced the government’s ability to “encroach on areas normally guarded from inquisitive eyes.” He cites to both *Kyllo v. United States* (which held that warrant was required for the government to use a thermal imaging device on a home) and *Riley v. California* (which held that a warrant was generally required to search the contents of a cell phone) to illustrate the ways in which changes in technology have necessitated an approach more nuanced than a “‘mechanical interpretation’ of the Fourth Amendment.”

Addressing the facts of this case, Chief Justice Roberts writes that CSLI does not “fit neatly under existing precedents,” and that it instead lies at the “intersection of two lines of cases”—the first line addressing geolocation, and the second addressing the third-party doctrine.

He begins with a discussion of the geolocation cases. He distinguishes *United States v. Knotts*, in which the court held that a warrant was not required to follow simple beeper placed in a suspect’s car, from *Jones*, in which the court held that a warrant was required for the placement of GPS device. In *Knotts*, the court found that the device simply augmented the police’s ability to track an individual’s public movements, while in *Jones*, the police used “more sophisticated surveillance” to track “‘every movement’ a person makes in that vehicle.” Roberts quotes Justice Alito’s *Jones* concurrence, noting that “longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.”

Roberts then discusses the third-party doctrine, addressing both *Miller* (which found that no expectation of privacy exists for bank records) and *Smith* (which found the same for phone company records of outgoing numbers dialed). Roberts highlights the court’s reasoning in *Smith*, noting that “[w]hen Smith placed a call, he ‘voluntarily conveyed’ the dialed numbers to the phone company by ‘expos[ing] that information to its equipment in the ordinary course of business.’”

Roberts then turns to the analysis of the question at hand: whether a warrant is required to access CSLI. He immediately highlights the potential privacy impact of CSLI, noting that “[m]uch like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled,” and distinguishes CSLI from the data in the third-party line of cases. “After all,” he points out “when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person’s movements.”

Roberts expressly declines to extend the third-party doctrine to CSLI. “Given the unique nature of cell phone location records,” he states, “the fact that the information is held by a third party does not by itself overcome the user’s claim to Fourth Amendment protection.”

Instead, he holds “that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter’s wireless carriers was the product of a search.”

In a footnote, Roberts notes that that court does not specifically hold on whether fewer days of CSLI could be accessed without a warrant (a weeks’ worth of records were accessed in Carpenter). “[W]e need not decide whether there is a limited period for which the Government may obtain an individual’s historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.”

Roberts then explains why there is a reasonable expectation of privacy in CSLI, beginning with the privacy interest in location data. He references the concurrences in *Jones* once again to support the proposition that it is reasonable for society to expect that law enforcement will not catalogue an individual’s every movement. With respect to CSLI, he points out that “the time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’”

CSLI, Roberts states, presents an “even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*,” because a cell phone is almost a “feature of human anatomy” (quoting *Riley*) and “tracks nearly exactly the movements of its owner.” Further, he notes that the “the retrospective quality of the data here gives police access to a category of information otherwise unknowable,” pointing out that the only real limit on the government’s ability to gather information is the length of time the data is retained by wireless carriers “which currently maintain records for up to five years.”

Roberts goes on:

Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government’s view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.

The government argued that the CSLI obtained in this particular case was less precise than GPS information. But Roberts notes that CSLI accuracy is “rapidly approaching GPS-level precision,” and emphasizes the language in *Kyllo* that the courts “must take account of more sophisticated systems that are already in use or in development.”

Roberts then explains why the third-party doctrine does not extend to this data. He notes that “seismic shifts in digital technology” have made it possible for constant location data to be collected on all cellphone users for years. “There is a world of difference,” he writes, “between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.”

The bank data in *Miller* and pen register data in *Smith*, Roberts explains, had a limited ability to reveal sensitive information. But “there are no comparable limitations on the revealing nature of CSLI.” He addresses the concerns of the dissenting justices who were skeptical of the sensitivity of this data, writing that “this case is not about ‘using a phone’ or a person’s movement at a particular time. It is about a detailed chronicle of a person’s physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*.”

Roberts also distinguishes *Smith* and *Miller* on voluntariness grounds. “Cell phone location information is not truly ‘shared’ as one normally understands the term,” he explains. Not only is a cell phone “indispensable to participation in modern society,” but a “cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up.” Because of this, Roberts concludes that “[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data,” meaning that the user does not voluntarily assume the risk of sharing the data.

Roberts concludes his analysis by explaining that the decision is “a narrow one.” He clarifies that the Court is not disturbing “the application of *Smith* and *Miller*,” or “call[ing] into question conventional surveillance techniques and tools, such as security cameras,” or “business records that might incidentally reveal location information.”

Finally, Roberts holds that a warrant is required for CSLI, and that “an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records.” He addresses concerns raised by Justice Alito in his dissent that a court order is typically sufficient to access records, noting that while this is true when there is a diminished expectation of privacy in the records, it is not true in this case, because “CSLI is an entirely different species of business record.” He notes that this is not a far-reaching conclusion, stating that law enforcement “will be able to use subpoenas to acquire records in the overwhelming majority of investigations.”

Roberts also notes that existing exceptions to the warrant requirement, such as the existence of exigent circumstances, will still apply to CSLI. “While police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation,” he explains “the rule we set forth does not limit their ability to respond to an ongoing emergency.”

Roberts concludes by emphasizing once again “the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection,” writing that “the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.”

Dissents

The four dissenting justices each filed separate opinions. Justices Thomas and Alito both joined Justice Kennedy’s opinion, and Justice Thomas joined Justice Alito’s opinion.

Justice Kennedy

Justice Kennedy dissents primarily on third-party doctrine grounds, arguing that CSLI is not fundamentally different from other business records, and that the 2703(d) orders were all law enforcement needed to access them. “Cell-site records,” he writes, “are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process.” He finds the distinction Roberts draws between CSLI and other phone or credit card records to be “illogical.”

Notably, Kennedy’s description of the accuracy of CSLI differs starkly from that of Roberts. Where Roberts focuses on current CSLI as approaching GPS levels of accuracy, Kennedy states that “cell-site records reveal the general location of the cell phone user,” and that they can “reveal the location of a cell phone user within an area covering between around a dozen and several hundred city blocks.”

Kennedy emphasizes the routine business nature of the records, and their importance to wireless service providers. He notes that providers aggregate and sell this data to third parties, and that the “market for cell phone data is now estimated to be in the billions of dollars.” He also notes the important role CSLI plays in criminal investigations, explaining that this data is “uniquely suited” to the task of linking the criminal gang in this case to the specific robberies they were suspected to have committed.

Kennedy argues that no search within the meaning of the Fourth Amendment occurred in this case. Because, he argues, the records were controlled by a third party, Carpenter lacked a privacy interest in them, and no search occurred in acquiring the CSLI from the wireless providers. He relies on both *Miller* and *Smith* to argue that the property-based conceptions of the Fourth Amendment still apply—that “individuals often have greater expectations of privacy in things and places that belong to them, not to others.” In *Miller* and *Smith*, Kennedy argues, the defendants “could make no argument that the records were their own papers or effects.” The records in *Miller* and *Smith* “were the business entities’ records, plain and simple,” and the defendants in those cases “had no reason to believe the records were owned or controlled by them and so could not assert a reasonable expectation of privacy in the records.”

Kennedy then turns to the sufficiency of a compulsory process (a court order requiring a lower standard of suspicion than a warrant). He explains the difference, noting that “[w]hile a warrant allows the Government to enter and seize and make the examination itself, a subpoena simply requires the person to whom it is directed to make the disclosure.” When a defendant has no privacy interest in the records, as was the case in *Miller* and *Smith*, the defendant has no right to object to its disclosure.

Kennedy then describes a number of situations in which a subpoena has been found to be sufficient, noting “it is well established that subpoenas maybe used to obtain a wide variety of records held by businesses, even when the records contain private information.” He cites credit card records, vehicle registration records, hotel records, employment records, and utility records as examples.

Kennedy argues that Carpenter is like the defendants in *Miller* and *Smith*, noting that he “can ‘assert neither ownership nor possession’ of the records and has no control over them.” He dismisses Carpenter’s argument that 47 U.S.C. § 222 grants customers an interest in CSLI as their “personal papers,” noting that the “statute’s confidentiality protections may be overridden by the interests of the providers or the Government.” He continues, “[c]ustomers do not create the records; they have no say in whether or for how long the records are stored; and they cannot require the records to be modified or destroyed. Even their right to request access to the records is limited.”

For these reasons, Kennedy argues, “Carpenter lacks a requisite connection to the cell-site records,” and he therefore “may not claim a reasonable expectation of privacy in them.” Kennedy argues that it would have been reasonable for Carpenter to expect that his wireless provider would “use the information it collected, stored, and classified as its own for a variety of business and commercial purposes.”

Kennedy then proceeds with his analysis of the majority opinion. He addresses the geolocation cases (*Knotts* and *Jones*), pointing out that while the court in *Knotts* suggested that its holding would not apply to “dragnet-type law enforcement practices,” this meant “twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision,” and that in this case, there was a “judicial

check,” because a magistrate judge issued the 2703(d) orders. He also rejects the majority’s adoption of the concurring opinions in *Jones*, noting that in *Jones*, the Court’s holding was that that a search had occurred because the police “physically occupied private property [of the defendant] for the purpose of obtaining information,” and that there had been no court-approved compulsory process in that case.

Kennedy goes on to criticize the majority’s treatment of *Miller* and *Smith*. He writes that in his view, the majority opinion appears to read those cases as establishing a balancing test, weighing “the privacy interests at stake” against “the fact that the information has been disclosed to a third party.” Kennedy rejects this reading, stating that “the fact that information was relinquished to a third party was the entire basis for concluding that the defendants in those cases lacked a reasonable expectation of privacy.”

Even if the balancing test is the way to address the third-party doctrine, Kennedy believes that “the Court errs . . . when it concludes that cell-site records implicate greater privacy interests—and thus deserve greater Fourth Amendment protection—than financial records and telephone records.” He argues that “a person’s movements are not particularly private,” stating that “[t]oday expectations of privacy in one’s location are, if anything, even less reasonable than when the Court decided *Knotts*.” He once again points to the accuracy of the CSLI in this case, noting that it “could not reveal where Carpenter lives and works, much less his “familial, political, professional, religious, and sexual associations.” He also draws similarities between the intimacy of location information and the intimacy of the data in financial and telephone records, as well as similarities in their retrospective reach, and the need to provide this information to third parties to participate in society.

Finally, Kennedy addresses the majority’s emphasis on the march of technology, writing that “future developments are no basis upon which to resolve this case.” He argues that the Court “risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society becomes clear.” He cites Orin Kerr’s equilibrium adjustment theory, explaining that new technology can make both criminal activity and law enforcement easier, and the balance “often will be difficult to determine during periods of rapid technological change.” He notes that Congress has weighed in on this issue through the SCA, and that “[t]he last thing the Court should do is incorporate an arbitrary and outside limit . . . and use it as the foundation for a new constitutional framework.”

In criticizing the majority’s opinion, Kennedy notes that CSLI is an important investigative tool, and that imposing a warrant requirement will “the effectiveness of an important investigative tool for solving serious crimes.” He notes that CSLI is well suited to helping law enforcement “develop probable cause to apprehend some of the Nation’s most dangerous criminals.” He also writes that the Court did not explain “what makes [CSLI] a distinct category of information,” and that the “the majority opinion gives courts and law enforcement officers no indication how to determine whether any particular category of information falls on the financial-records side or the cell-site-records side of its newly conceived constitutional line.”

Kennedy also criticizes the majority opinion suggestion that “that less than seven days of location information may not require a warrant,” noting that “nothing in its opinion even alludes to the considerations that should determine whether greater or lesser thresholds should apply to information like IP addresses or website browsing history.” He also notes that the majority leaves open questions of how the decision will affect “the subpoena practices of federal and state grand juries, legislatures, and other investigative bodies.”

Kennedy concludes by arguing that when the majority reached the conclusion that the acquisition of Carpenter’s CSLI was a search, it should have remanded to the Sixth Circuit to “to ‘determine in the first instance whether the search was reasonable.’ Finally, he states that “the Court’s reflexive imposition of the warrant requirement obscures important and difficult issues, such as the scope of Congress’ power to authorize the Government to collect new forms of information using processes that deviate from traditional warrant procedures, and how the Fourth Amendment’s reasonableness requirement should apply when the Government uses compulsory process instead of engaging in an actual, physical search.”

Justice Thomas

Justice Thomas’ dissent begins with a clear thesis. “This case should not turn on ‘whether’ a search occurred,” he states. “It should turn, instead, on whose property was searched.” In *Carpenter*, he argues, the CSLI records “belong to MetroPCS and Sprint.” He goes a step further than Kennedy, arguing that the reasonable-expectation-of-privacy test “has no basis in the text or history of the Fourth Amendment. And, it invites courts to make judgments about policy, not law.”

Thomas begins with a history of wiretap jurisprudence and its origins in trespass theory, beginning with *Olmstead*, a 1928 case in which the court held that placing an electronic eavesdropping device was not a search because it was placed without physical entry into the defendant’s home. He notes that the court relied on *Olmstead* until the 1960s. First, the court in *Silverman* held that a microphone placed through the wall of a home was a search, without relying on *Olmstead*’s assertion that “intangible conversations are not ‘persons, houses, papers, [or] effects.’” Thomas notes that the *Katz* decision in 1967 “rejected *Olmstead*’s remaining holding—that eavesdropping is not a search absent a physical intrusion into a constitutionally protected area.”

Thomas then critiques the *Katz* holding, and the notion that the question of whether a search occurred turns on whether a reasonable expectation of privacy was violated, not on “the presence or absence of a physical intrusion.” Thomas notes that the two-pronged reasonable-expectation-of-privacy test, which looks to society’s expectations and the individual’s subjective expectations in determining whether a privacy interest exists, was presented for the first time during the *Katz* oral argument by a “recent law-school graduate.” He explains that, following *Katz*, the two-pronged test was adopted almost immediately, and over time, the subjective prong has been minimized, leaving reasonable societal expectations (the objective prong) as the dispositive factor in Fourth Amendment jurisprudence.

Thomas argues that the reasonable expectation of privacy test “has ‘no plausible foundation in the text of the Fourth Amendment.’” He quotes the text of the Fourth Amendment, which describes “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches,” and argues that “the *Katz* test misconstrues virtually every one of these words.” At the founding, Thomas argues, “search” did not “mean a violation of someone’s reasonable expectation of privacy.” Instead, it held the same plain meaning that it does today “[t]o look over or through for the purpose of finding something; to explore; to examine by inspection.”

Further, Thomas notes, the word “privacy” does not appear in the Fourth Amendment. Instead, “[t]he text of the Fourth Amendment reflects its close connection to property.” At the founding, Thomas argues, “liberty and privacy rights were understood largely in terms of property rights.” He cites to John Locke’s *Second Treatise of Civil Government*, and the English case *Entick v. Carrington* to support his argument that privacy is security in property. He argues that by “shifting the focus of the Fourth Amendment from property to privacy, the *Katz* test also reads the words ‘persons, houses, papers, and effects’ out of the text,” and argues that this misunderstood the Fourth Amendment’s original purpose.

Next, Thomas turns to the issue of ownership, stating that the constitution “specifies that the people have a right to be secure from unreasonable searches of ‘their’ persons, houses, papers, and effects,” explaining that it should mean that “individuals do not have Fourth Amendment rights in someone else’s property.” However, Thomas notes, under the *Katz* test, the court has found that there can be a privacy interest in someone else’s property—like someone else’s home.

Thomas then addresses Carpenter’s cell-site location information. He argues that Carpenter’s claim that the CSLI qualifies as his “papers” within the meaning of the Fourth Amendment is “unpersuasive.” Thomas notes that no statutes nor Carpenter’s contracts with the wireless providers render the data his property. Thomas rejects Carpenter’s argument that the privacy provisions of Section 222 of Title 7 of the U.S. code grant him any privacy interest because the statute does not give him ownership of the records.

Next, Thomas addresses the reasonableness aspect of the *Katz* test. He writes “reasonableness determines the legality of a search, not ‘whether a search . . . within the meaning of the Constitution has occurred.’” Citing Laura Donahue, he explains that “the word ‘unreasonable’ in the Fourth Amendment likely meant ‘against reason’—as in “against the reason of the common law.” Rather than protecting societal expectations of reasonableness he argues, “by prohibiting ‘unreasonable’ searches and seizures in the Fourth Amendment, the Founders ensured that the newly created Congress could not use legislation to abolish the established common-law rules of search and seizure.”

The Founders, Thomas argues, “would be puzzled by the Court’s conclusion as well as its reasoning.” He writes that to the Founders, “a subpoena for third-party documents was not a ‘search’ to begin with, and the common law did not limit the government’s authority to subpoena third parties.” They would “be confused by this Court’s transformation of their common-law protection of property into a ‘warrant requirement’ and a vague inquiry into ‘reasonable expectations of privacy.’”

In his final section, Thomas critiques the *Katz* test for being “unworkable in practice.” One issue is that “[a]s written, the *Katz* test turns on society’s actual, current views about the reasonableness of various expectations of privacy,” which renders it “easily circumvented.” Thomas cites to Chemerinsky in noting that the government could, in theory, “deny privacy just by letting people know in advance not to expect any.” Thomas also notes that the court has never adequately defined “understandings that are recognized or permitted in society.”

Finally Thomas criticizes the court for treating the *Katz* test as “a normative question—whether a particular practice should be considered a search under the Fourth Amendment,” noting that the court’s precedents “bear the hallmarks of subjective policymaking instead of neutral legal decisionmaking.” Thomas concludes his dissent by describing the *Katz* test as a “failed experiment” and implores the court to reconsider it.

Justice Alito

Justice Alito begins by noting that while he shares concerns about the “effect of new technology on personal privacy,” the majority’s reasoning “fractures two fundamental pillars of Fourth Amendment law, and in doing so, it guarantees a blizzard of litigation while threatening many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely.”

Alito's dissent focuses on two issues: the distinction between a search and an order requiring the disclosure of documents, and the fact that CSLI is the property of the service provider. "By departing dramatically from these fundamental principles," Alito writes "the Court destabilizes long-established Fourth Amendment doctrine."

Alito begins with his analysis of the warrant requirement. "The Court's holding is based on the premise that the order issued in this case was an actual 'search' within the meaning of the Fourth Amendment," Alito writes, "but that premise is inconsistent with the original meaning of the Fourth Amendment and with more than a century of precedent."

Justice Alito then outlines a brief history of the subpoena, beginning with writs of subpoena issued under the reign of King Richard II in the late 14th century. He describes a shift in the primary use of the subpoena to compel presence or testimony, to the widespread use of the subpoena *duces tecum* to compel the production of papers, books, and other forms of physical evidence.

Alito tracks the use of the subpoena to the United States, pointing out that through the Judiciary act of 1789, the First Congress authorized the courts to "compel the production of papers, books, and other forms of physical evidence, whether from the parties to the case or from third parties." He notes that subpoenas were used regularly to compel the production of documents in criminal cases in the founding era. He points to the prevalence of grand juries to argue that "the Founders must have been intimately familiar with the tools they used" including the subpoena *duces tecum*.

The history matters, Alito argues, "not least because it tells us what was on the minds of those who ratified the Fourth Amendment and how they understood its scope. That history makes it abundantly clear that the Fourth Amendment, as originally understood, did not apply to the compulsory production of documents at all." Because the "compulsory production of documents" is "a practice that involves neither any physical intrusion into private space nor any taking of property by agents of the state," the Fourth Amendment does not apply.

Alito continues discussing the history, noting that the Fourth Amendment "was the founding

generation's response to the reviled 'general warrants' and 'writs of assistance.'" Because a "subpoena *duces tecum* permits a subpoenaed individual to conduct the search for the relevant documents himself, without law enforcement officers entering his home or rooting through his papers and effects ... subpoenas avoid the many incidental invasions of privacy that necessarily accompany any actual search." The Founders, he continues "would thus have understood that holding the compulsory production of documents to the same standard as actual searches and seizures would cripple the work of courts in civil and criminal cases alike."

Justice Alito then acknowledges that the court has held that subpoenas to produce documents can violate the Fourth and Fifth Amendments, citing to an 1886 decision, *Boyd v. United States*, in which the court found an order "unconstitutional because it compelled the production of property to which the Government did not have superior title." Alito notes that the reasoning in *Boyd* was "confused from start to finish in a way that ultimately made the decision unworkable."

Alito tracks the development of the law surrounding subpoenas *duces tecum* through to *Oklahoma Press Publishing Co. v. Walling*, a 1946 case in which the court found that "the Fourth Amendment regulates the compelled production of documents, but less stringently than it does full-blown searches and seizures," and that the distinction between searches and compulsory orders "meant that two different standards had to be applied." For a subpoena, Justice Alito explains, the *Oklahoma Press* court held that "a showing of probable cause was not necessary so long as "the investigation is authorized by Congress, is for a purpose Congress can order, and the documents sought are relevant to the inquiry."

Justice Alito then turns to the application of this doctrine to CSLI. Alito agrees with Justice Kennedy that "no search or seizure of Carpenter or his property occurred in this case." He states that the 2703(d) order clearly meets the *Oklahoma Press* standard.

Justice Alito then critiques the majority opinion for "imposing requirements that—until this point—have governed only actual searches and seizures." To the majority, Alito argues "this case is apparently no different from one in which Government agents raided Carpenter's home and removed records associated with his cell phone."

Alito continues along this line of reasoning, pointing out that the majority does not "explain why that individual should be entitled to greater Fourth Amendment protection than the party actually being subpoenaed." He argues that this "outcome makes no sense, and the Court does not even attempt to defend it." Holding "that subpoenas must meet the same standard as conventional searches," Alito concludes, "will seriously damage, if not destroy, their utility."

Alito then turns to the second issue he identifies: whether "a defendant has the right under the Fourth Amendment to object to the search of a third party's property." In an analysis that mirrors Kennedy's dissent, Alito argues that the CSLI records "belong to Carpenter's cell service providers, not to Carpenter." Alito explains that because Carpenter had "no meaningful control over the cell-site records," and that the Telecommunications Act ([47 U.S.C. § 222](#)) provides no basis for a property right in the data, "there is no plausible ground for maintaining that the information at issue here represents Carpenter's 'papers' or 'effects.'"

Alito then turns to the third-party doctrine, addressing *Miller* and *Smith*. He agrees with Kennedy that this line of cases is best understood as placing “limits on the ability of individuals to assert Fourth Amendment interests in property to which they lack a ‘requisite connection.’” Because “Carpenter indisputably lacks any meaningful property-based connection to the cell-site records owned by his provider,” Alito concludes that Carpenter “may not seek to use the Fourth Amendment to exclude them.”

Concluding his dissent, Alito speculates on the effect the majority opinion will have on the use of the subpoena. “One possibility” he suggests “is that the broad principles that the Court seems to embrace will be applied across the board. All subpoenas duces tecum and all other orders compelling the production of documents will require a demonstration of probable cause.” Another is “that this Court will face the embarrassment of explaining in case after case that the principles on which today’s decision rests are subject to all sorts of qualifications and limitations that have not yet been discovered.”

Finally, he stresses that this issue was already addressed by legislation. The SCA “restricts the misuse of cell-site records by cell service providers, something that the Fourth Amendment cannot do.” He argues that legislation is a better way to address technological change, writing that it “is much preferable to the development of an entirely new body of Fourth Amendment case law for many reasons, including the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment’s limited scope.”

“The desire to make a statement about privacy in the digital age,” he writes “does not justify the consequences that today’s decision is likely to produce.”

Justice Gorsuch

Justice Gorsuch structures his dissent around three possible solutions to the problems of the reasonable expectation of privacy test. First, “ignore the problem, maintain *Smith* and *Miller*, and live with the consequences.” Second, set *Smith* and *Miller* aside and try again using the *Katz* ‘reasonable expectation of privacy’ jurisprudence that produced them.” The third solution, Gorsuch suggests, “is to look for answers elsewhere.”

Gorsuch begins with the solution of maintaining *Smith* and *Miller*. He agrees with Justice Kennedy’s criticism of the majority’s proposed balancing test. *Smith* and *Miller* “announced a categorical rule,” he writes: “Once you disclose information to third parties, you forfeit any reasonable expectation of privacy you might have had in it.” He also questions the majority’s finding that location information is more sensitive than numbers dialed or financial records.

Gorsuch then criticizes *Smith* and *Miller*, and the third-party doctrine generally. “Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights?” Gorsuch asks. “Can it secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can.” He indicates doubt in the premise of the third-party doctrine, noting that if it is “supposed to represent a normative assessment of when a person should expect privacy, the notion that the answer might be “never” seems a pretty unattractive societal prescription.”

Gorsuch then proceeds to analyze the development of the third-party doctrine. He addresses the “assumption of risk” model, which finds its roots in tort law. He argues that the rationale of the tort law model “has little play in this context,” and notes that even in tort law, “knowing about a risk doesn’t mean you assume responsibility for it.” He also discusses consent theories of the third-party doctrine, arguing that “[c]onsenting to give a third party access to private papers that remain my property is not the same thing as consenting to a search of those papers by the government” (emphasis in original). He argues that *Smith* and *Miller* ultimately stand for the proposition that *Katz* “lets the government search almost whatever it wants whenever it wants.”

He then turns to the second option—returning to “the root *Katz* question whether there is a ‘reasonable expectation of privacy’ in data held by third parties.” This option, Gorsuch concludes, does not solve any problems. Like Thomas, Gorsuch discusses the text of the Fourth Amendment, and notes that its “protections do not depend on the breach of some abstract ‘expectation of privacy’ whose contours are left to the judicial imagination.”

Like Thomas, Gorsuch looks to the history of the Fourth Amendment, noting that 18th century cases addressing general warrants and writs of assistance prompted the Founders to address privacy protections. The Founders, Gorsuch notes “chose not to protect privacy in some ethereal way dependent on judicial intuitions. They chose instead to protect privacy in particular places and things—‘persons, houses, papers, and effects’—and against particular threats—‘unreasonable’ governmental ‘searches and seizures.’”

He highlights other problems with the reasonable expectation of privacy test, noting that it is unclear whether it is intended to pose an empirical question or a normative one. Regardless of whether it is an empirical or normative test, Gorsuch questions “why judges rather than legislators should conduct it.” He argues that the legislature is better suited to answer these questions noting that “answering questions like that calls for the exercise of raw political will belonging to legislatures, not the legal judgment proper to courts.”

Gorsuch does not deny that judges may sometimes “be able to discern and describe existing societal norms,” but argues that the Court has yet to tie itself to any particular principled application of *Katz*. He discusses a few Fourth Amendment cases that produced results he considers “unpredictable—and sometimes unbelievable” including *Florida v. Riley* in which the court found no reasonable expectation of privacy from a helicopter flying 400 feet above a person’s property, and *California v. Greenwood* in which the Court found no reasonable expectation of privacy existed in garbage put out for collection.

With respect to data privacy in particular, Gorsuch argues that relying on *Katz* will lead to continued unpredictable results. He criticizes the majority opinion for not supplying lower courts with significant guidance, noting that it did not address “whether there is any sufficiently limited period of time” for which CSLI can be obtained without a warrant.

Gorsuch also raises questions about the majority silence on real-time CSLI and tower dumps, asking “what distinguishes historical data from real-time data, or seven days of a single person’s data from a download of everyone’s data over some indefinite period of time?” Gorsuch also criticizes the majority for creating “a second *Katz*-like balancing inquiry, asking whether the fact of disclosure to a third party outweighs privacy interests in the ‘category of information’ so disclosed.”

In summing up the first two solutions, Gorsuch notes that they leave lower courts “with two amorphous balancing tests, a series of weighty and in-commensurable principles to consider in them, and a few illustrative examples that seem little more than the product of judicial intuition.”

Gorsuch then turns to the third solution—looking for guidance elsewhere. Unsurprisingly given his line of questioning at oral argument, he finds this guidance in property law. “We know that if a house, paper, or effect is yours, you have a Fourth Amendment interest in its protection” he notes. “But what kind of legal interest is sufficient to make something *yours*?” Gorsuch does not “begin to claim all the answers” but raises a series of questions with which to address the issue.

First, he turns to the concept of bailments to argue that “the fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them.” He quotes the *Black’s Law Dictionary* definition, which defines bailments as “delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose.” He cites to *Ex parte Jackson*, which found a privacy interest in the contents of sealed letters in the mail, to support the proposition that this idea is already reflected in Fourth Amendment jurisprudence. “Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party,” Gorsuch argues “may not mean you lose any Fourth Amendment interest in its contents.”

“[C]omplete ownership or exclusive control of property,” Gorsuch continues, is not “always a necessary condition to the assertion of a Fourth Amendment right.” He notes that individuals may have a privacy interest in a home they do not own, even when they “merely occupy it for free.”

Gorsuch also argues that “just because you have to entrust a third party with your data doesn’t necessarily mean you should lose all Fourth Amendment protections in it,” and analogizes the storage of data with third parties to an involuntary bailment, as in cases of lost goods being found, or the contents of an impounded car.

Next, Gorsuch looks to the Takings Clause, which often requires courts to ask whether those state-created rights in tangible and intangible things “are sufficient to make something someone’s property for constitutional purposes.” He suggests that “[a] similar inquiry may be appropriate for the Fourth Amendment.” Pointing to state court opinions and legislation, he notes that “state legislators or state courts say that a digital record has the attributes that normally make something property, that may supply a sounder basis for judicial decisionmaking than judicial guesswork about societal expectations.”

Gorsuch also argues that although positive law can help to establish a Fourth Amendment interests, “there may be some circumstances where positive law cannot be used to defeat it.” He argues that “[l]egislatures cannot pass laws declaring your house or papers to be your property except to the extent the police wish to search them without cause.”

Finally, Gorsuch notes that the Fourth Amendment’s protections cannot be evaded through the use of subpoenas. “No one thinks the government can evade *Jackson*’s prohibition on opening sealed letters without a warrant,” Gorsuch posits “simply by issuing a subpoena to a postmaster for ‘all letters sent by John Smith.’” Courts will need to address “[w]hat other kinds of records are sufficiently similar to letters in the mail that the same rule should apply.” Gorsuch does not have an answer to this question, indicating that he is “content to adhere to *Jackson* and its implications for now,” although he also warns against restricting the use of subpoenas.

Concluding his dissent, Gorsuch states that he does not “agree with the Court’s decision today to keep *Smith* and *Miller* on life support and supplement them with anew and multilayered inquiry that seems to be only *Katz*-quared.” He suggests looking to a “more traditional Fourth Amendment approach,” and laments the fact that Carpenter did not pursue a line of argument based on property rights and positive law. “I cannot help but conclude—reluctantly—that Mr. Carpenter forfeited perhaps his most promising line of argument.”

Final Notes

Notably, this result should have little effect on Timothy Carpenter's future. Under the good faith doctrine, established by *United States v. Leon*, evidence cannot be suppressed at trial when law enforcement relies on a defective court order in good faith. In this case, even though the 2703(d) orders have been deemed insufficient to access CSLI, the police relied on them in good faith—so the suppression remedy is not available to Carpenter. The case has been remanded to the Sixth Circuit, but this decision is unlikely to have any impact on Carpenter's convictions.

Topics: U.S. Supreme Court, Fourth Amendment

Sabrina McCubbin graduated cum laude from Georgetown University Law Center, where she was the student editor-in-chief of the Journal of National Security Law and Policy. She has worked at the Center for Strategic and International Studies and the Center on Privacy and Technology. She earned her B.A. from McGill University in 2012.

 **SabrinaMcCubbin**

 This work is licensed under a Creative Commons Attribution 4.0 International License.

THE COST OF PRIVACY: *RILEY V. CALIFORNIA'S* IMPACT ON CELL PHONE SEARCHES

Jennifer L. Moore, Jonathan Langton, and Joseph Pochron
DeSales University
2755 Station Avenue, Center Valley, Pennsylvania 18034
jennifer.moore@desales.edu

ABSTRACT

Riley v. California is the United States Supreme Court's first attempt to regulate the searches of cell phones by law enforcement. The 2014 unanimous decision requires a warrant for all cell phone searches incident to arrest absent an emergency. This work summarizes the legal precedent and analyzes the limitations and practical implications of the ruling. General guidelines for members of the criminal justice system at all levels consistent with the Supreme Court's decision are provided.

Keywords: search incident to arrest, cell phone searches, U.S. Supreme Court

1. INTRODUCTION

The law notoriously lags behind advancements in technology. The initial explosion of cybercrimes in the 21st century left the American criminal justice system woefully unprepared. The courts struggled to confront the emerging crimes of computer hacking, Internet viruses and sexting with traditional criminal statutes. Forced to work within the confines of criminal laws already on the books, trespass, theft and child pornography statutes were stretched to new limits (Birkhold, 2013). While the federal and state governments eventually updated their laws, the technology gap remains.¹ The slow response time of state and federal legislatures perpetuates a legal system constantly trying

to "catch up" with innovation. In addition, a two hundred year old constitution is also asked to confront modern technological issues that the founding fathers never imagined. The long delay in the appellate process further exasperates the technological gap, as the Supreme Court just addressed the now outdated use of pagers in 2010 (*City of Ontario v. Quon*, 2010).

The search and seizure clause of the Fourth Amendment was recently evaluated in relation to cell phone privacy. Nearly 41 years after the development of the first mobile phone ("The first mobile", 2013), the Supreme Court in *Riley v. California* issued its first major privacy ruling regarding the devices. In a unanimous decision, the justices emphatically ruled that the search of a suspect's cell phone incident to arrest requires a warrant. Conceding that *Riley* will now make the job of law enforcement more difficult, the Court emphasized the unique attributes of cell phones and the cost of maintaining personal privacy (*Riley v.*

¹ See The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2008); Pennsylvania enacted its sexting statute on October 25, 2012 in 18 P.A.C.S. § 6312 (2014).

California, 2014). Local, state and federal law enforcement agencies must now confront the real-world impact of *Riley* in criminal investigations. This article will examine the legal aspects of the Supreme Court's opinion in *Riley* and highlight the limitations of the ruling. In addition, the practical effect of the decision on various parties in the criminal justice system will be evaluated in detail. Finally, a blueprint of acceptable digital forensic techniques after *Riley* will be explained.

2. THE SUPREME COURT'S UNANIMOUS VERDICT

The Supreme Court consolidated the cases of David Leon Riley and Brima Wurie in a groundbreaking case regarding the evolution of privacy in the digital age. In separate incidents, both men had their cell phones searched incident to arrest without a warrant. The information contained on their cell phones ultimately led to convictions for additional offenses. Riley was initially stopped in California for a traffic violation but eventually arrested after an inventory search revealed two loaded handguns under the hood of his car. During the search incident to arrest, Riley's cell phone was removed from the pocket of his pants and searched preliminarily by the police officer on scene. A review of texts messages and contacts indicated membership in the Bloods street gang. Two hours after the arrest, a detective further analyzed Riley's cell phone without a warrant at the police station. The detective discovered photographs of Riley standing near a car allegedly used in a drive by shooting. Riley was ultimately convicted for attempted murder, assault with a semiautomatic firearm, and firing at an occupied vehicle and sentenced to 15 years to life in prison for his involvement in the drive by shooting (*Riley v. California*, 2014, p. 2481).

Brima Wurie was arrested after purchasing drugs and two cell phones were seized from his person incident to arrest. At the police station, Burie's phone continued to receive calls from a contact noted as "my house." An officer opened the flip phone and accessed the call log to retrieve the incoming telephone number. A trace of the number was completed to obtain a physical address. After securing a search warrant, the police searched Burie's home and seized weapons, cash and large amounts of crack cocaine. Burie's convictions resulted in a sentence of 262 months in federal prison (*Riley v. California*, 2014, p. 2482). On appeal, both cases raised the question of whether a warrant is needed to search a cell phone incident to arrest.

Chief Justice Robert's opinion addressed the question presented within the framework provided by the leading search incident to arrest case, *Chimel v. California*. In 1969, *Chimel* declared that police officers could perform a warrantless search of a suspect and the area within the suspect's immediate control incident to an arrest. This exception to the warrant requirement was justified by the potential threat to officer safety and the possibility for the destruction of valuable evidence (*Chimel v. California*, 1969). The *Chimel* doctrine was extended to include a quick search of personal property "immediately associated with the person of the arrestee" (*U.S. v. Chadwick*, 1977, p. 15). In searching for relevant precedent applicable to the factual scenarios before the Court, Chief Justice Roberts focused on the 1973 decision of *United States v. Robinson*. The holding in *Robinson* permitted police officers to search a crumpled cigarette packet located in a suspect's coat pocket incident to arrest. A review of the contents of the cigarette packet revealed illegal drugs. The Supreme Court in *Riley* had to determine if a cell phone was analogous to that crumpled cigarette package or an entirely different category of property. Similar to most Fourth Amendment cases, the answer hinged on the balancing of government interests and individual privacy.

The unanimous decision spent a significant amount of time examining the unique characteristics of a cell phone. When compared to other physical objects, the Court emphasized the vast quantitative and qualitative differences of the modern phone. The immense storage capacity and variety of data contained on cell phones was emphasized, which Chief Justice Roberts noted could just “as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps or newspapers” (*Riley v. California*, 2014, p. 2489). Accordingly, a warrantless search of a cell phone implicates a substantially greater violation of privacy than reviewing the contents of a wallet or cigarette packet. The Court noted that 90 percent of adults in America essentially have “on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate” (*Riley v. California*, p. 2490). A detailed examination of a cell phone is analogous to an exhaustive search of an entire home.² Accordingly, cell phones were distinguished from other types of personal property and the precedent from *Robinson* was inapplicable.

The decision also reviewed each of the *Chimel* rationale as they applied to cell phones—officer safety and the imminent destruction of evidence. The Supreme Court quickly dismissed the concern for officer safety, noting that “[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee’s escape” (*Riley v. California*, 2014, p. 2485). While police officers remain free to examine the physical aspects of a cell phone for concealed risks, such as razor blades, the content of the phone remains protected. The Court also clarified that the

potential for “indirect” threats from third parties does not justify an automatic warrantless search of cell phone data incident to arrest. While data on a phone can potentially reveal to law enforcement that additional accomplices are en route to the scene, they are not covered by the rationale of *Chimel* and its progeny. *Chimel* applies only to threats from the arrestee, not third parties. In factually specific situations where a unique safety threat exists, the exigent circumstances exception remains available for law enforcement (*Riley v. California*, p. 2487).

In regards to the destruction of evidence rationale from *Chimel*, the Court focused on the potential for remote wiping or encryption of digital data. The federal government and the State of California argued that imminent threats to cell phone contents justified a warrantless search incident to arrest exception. Specifically, the contents of a phone can be completely erased if it remains connected to a wireless network and a third party sends the appropriate signal. In addition, after a phone locks the information stored can be encrypted with a special program to completely prevent access without the applicable encryption key. The Supreme Court quickly dismissed both ideas as justification for an automatic warrantless search, noting that little evidence was provided that these problems even exist in the field. The Court also reiterated that *Chimel* applies only to direct threats from the arrestee, and not to third parties wiping content or the normal functions of an encryption security feature. Police officers remain free to employ alternative methods to protect digital data at the scene of an arrest short of a search, such as removing the battery, turning the phone off or disabling an automatic-lock feature (*Riley v. California*, 2014).

² Chief Justice Roberts explained that, “a cell phone search would typically expose to the government to far more than the most exhaustive search of a house” (*Riley v. California*, 2014, p. 2491).

The unanimous Court concluded by acknowledging the impact of their decision, noting “[w]e cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime” (*Riley v.*

California, 2014, p. 2493). The decision in *Riley*, however, does not completely isolate a cell phone from a comprehensive search. It simply requires a warrant or an independent exception to the warrant requirement to justify the excessive privacy intrusion.

2.1 Justice Samuel Alito's Concurrence

While the Supreme Court was unanimous in requiring a warrant for cell phone searches incident to arrest, Justice Alito issued a concurrence to explain his legal reasoning. Specifically, the concurrence addressed the underlying *Chimel* rationale cited by the Court for conducting a search incident to arrest – officer safety and preventing the destruction of evidence. Alito argues that the practice of searching a suspect after an arrest has a strong historical foundation independent of the *Chimel* factors. Citing numerous historical examples of searches incident to arrest as routine practice for police officers, Alito concludes that “the rule is not closely linked to the need for officer safety and evidence preservation” (*Riley v. California*, 2014, p. 2496). In addition, Alito cites numerous court decisions that permitted officers to read written items found on suspects incident to arrest as evidence that safety and evidence destruction are not the only controlling factors. The concurrence clarifies that *Chimel* involved searching the scene of an arrest, not the search of a person. Accordingly, Alito would not “allow that reasoning to affect cases like these that concern the search of the person of the arrestees” (*Riley v. California*, p. 2496).

Alito also emphasizes the limits of the *Riley* decision and the need for state and federal legislatures to pass laws regarding digital evidence. Citing the passage of the Omnibus Crime Control Act after *Katz v. United States* restricted the warrantless monitoring of public pay phones, the concurrence emphasized the “better position” of legislatures to address changing technology. As written, Alito concedes that *Riley* gives

greater protection to digital evidence than physical evidence. An address on a slip of paper is searchable incident to arrest, but an address contained in a cell phone’s contacts list is not. Additionally, photographs in a wallet can be viewed by police officers, while those on a phone are protected. Alito concludes “it would be very unfortunate if privacy protection is the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment” (*Riley v. California*, 2014, p. 2497).

3. LIMITATIONS ON THE RULING

A single Supreme Court decision is never the “last word” on a specific legal issue. The opinion will inevitably be dissected by the lower courts, distinguished by different factual circumstances and interpreted differently. The *Riley* decision provides several notable limitations that can potentially impact police officers’ enforcement of the ruling. For example, the Roberts Court traditionally issues very limited decisions that apply specifically to the factual situations presented. *Riley* is no exception. Both consolidated cases resolved in *Riley* involved searches of cell phones incident to arrest. Consequently, the Court’s ruling appears to apply only in situations where the suspect is arrested. This leaves open the possibility for warrantless cell phone searches in other circumstances independent of arrest. For example, police may encounter a cell phone while performing a warrantless search under the automobile exception. Although the Supreme Court distinguished cell phones from other physical property, it did not completely eliminate the possibility that a brief content search might be appropriate in the automobile context due to the mobility of vehicles. In addition, the plain view exception could also arise and justify a cell phone search. If a police officer is lawfully in an apartment and sees a text message implicating criminal activity flash on the screen, they could be justified in searching

the phone. As long as the scenario does not involve a search incident to arrest, *Riley* is not completely controlling.

The opinion itself contains a limiting instruction to remind the audience that *Riley* is limited solely to search incident to arrest cases. In footnote 1, the Court notes that since both parties “agree that these cases involve *searches* incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances” (*Riley v. California*, 2014, p. 2489). Therefore, the collection of digital information by law enforcement using other means beyond cell phone examination incident to arrest remains an open legal issue.

Riley also fails to provide adequate guidance for limiting the scope of search warrants on cell phones. Mobile devices are currently searched and examined by practitioners with nuanced tools that contain forms of automated data extraction and parsing. While *Riley* calls for the acquisition of a search warrant, the Supreme Court did not specify which techniques could be used on mobile device. This issue has already surfaced in the lower courts. The U.S. District Court for the Central District of Illinois recently ruled in *U.S. v. Schlingloff* (2012) that a computer forensic practitioner may not utilize automated data filters to locate evidence that is extraneous to the basis of the probable cause articulated in the search warrant. In *Schlingloff*, a computer forensic practitioner utilized an automated filter within a forensic tool to search for files containing child pornography, resulting in the location of child pornography on the suspect’s computer. The warrant was explicitly based on probable cause pertaining to an identity theft investigation, and although the child pornography filter utilized to search the computer is commonly set as a default methodology within the forensic tool, the practitioner did have the ability to conduct an examination of the device without using the filter. Because the practitioner did not choose

to deactivate the child pornography filter, the District Court ruled that the utilization of the filter reached beyond the scope of the search, resulting in the suppression of the digital evidence. Although methodologies certainly differ between mobile device forensics and computer forensics, Chief Justice Roberts’ opinion in *Riley* draws clear analogies between modern cell phone technology and the capabilities that are typically associated with computers. Because of this commonality, *Schlingloff* may represent a glimpse into the future of legal issues concerning the examination of cell phones and the associated requirements for warrants and methodologies.

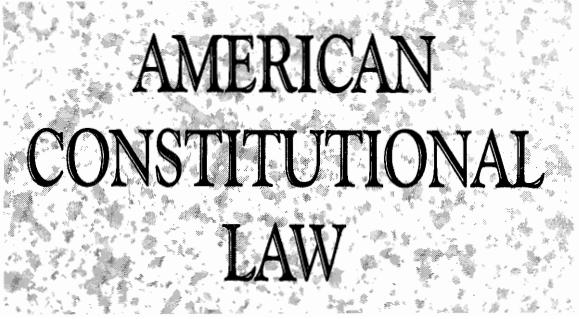
Although *Riley* largely neglected to delve into the intricacies of the scope of search warrants for digital devices, the Court acknowledged the complexities associated with the data capabilities of mobile devices. Just as Apple mobile devices support data storage through the iCloud service, modern cell phones consistently use data remotely stored on third-party servers. The Court explicitly referenced modern cell phones’ utilization of cloud computing, noting that “a cell phone is used to access data located elsewhere, at the tap of the screen” (*Riley v. California*, 2014, p. 2491). Although the majority opinion appears to recognize a necessity for Fourth Amendment protection of data stored through cloud-based technology, the Court hesitates to clearly delineate the important distinction between locally and remotely stored data. More importantly, *Riley* also fails to recognize the significance of such a distinction, stating that “cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference” (*Riley v. California*, p. 2491). While modern cell phone capabilities allow for the storage of data in a multitude of locations on the individual device and through cloud-based services, *Riley* fails to establish a framework for the legal and forensic interpretation of these differences. The Court’s opinion suggests that this distinction is irrelevant for the purpose of searching a device incident to arrest, and effectively paves

the way for further discussion and debate regarding the scope of warrants for the search of digital evidence.

Arguably, the *Riley* decision can also be read as applying only to cell phones as opposed to all types of electronic devices. While the type of information stored on a cell phone is analogous to that found on iPads or iPods, the justices did not directly make the comparison. As additional technological devices continue to emerge, such as Google glasses or the highly anticipated iWatch, courts will be forced to determine if they are similar enough to cell phones to apply *Riley*. An armband used by athletes to map their latest run or bike ride could provide indispensable GPS data. Since these devices lack the photographs, contacts, calendars and other personal information found on cell phones, they are potentially distinguishable from the *Riley* decision based on the level of privacy intrusion. The ultimate determination of what types of devices fall under *Riley's* control will fall on the lower courts.

The Supreme Court also expressly noted that the exigency exception to the warrant requirement is still applicable in appropriate factual circumstances to justify a search of cell phone data. Similar to other areas of Fourth Amendment jurisprudence, the warrant requirement is eliminated in situations where the safety of the police or public is in immediate danger or evidence is imminently being destroyed. The *Riley* opinion provides two factual examples in which a cell phone search may be justified due to exigent circumstances. First, law enforcement would be entitled to search the contents of a phone if the suspect is apparently texting an accomplice to detonate an explosive device. Second, the Court would seemingly allow the warrantless search of a phone believed to contain the location of a kidnapped child (*Riley v. California*, 2014, p. 2494). These examples simply highlight the potential for countless unique factual scenarios that justify cell phone searches

incident to arrest. As the lower courts begin to interpret and apply *Riley*, this exception possesses the greatest potential for expansion and abuse. At this time, however, the justices explicitly held that threats of remote wiping and/or data encryption do not constitute exigent circumstance.



AMERICAN CONSTITUTIONAL LAW

Otis H. Stephens, Jr.
John M. Scheb, II

Department of Political Science
University of Tennessee, Knoxville

Copyright © 1993 BY WEST PUBLISHING COMPANY

W E S T P U B L I S H I N G C O M P A N Y

Minneapolis/St. Paul • New York • Los Angeles • San Francisco

CASES AND READINGS

Olmstead v. United States

277 U.S. 438; 48 S. Ct. 564; 72 L. Ed. 944 (1928)

Vote: 5-4

Mr. Chief Justice Taft delivered the opinion of the court.

These cases are here by *certiorari* from the Circuit Court of Appeals for the Ninth Circuit. They were granted with the distinct limitation that the hearing should be confined to the single question whether the use of evidence of private telephone conversations between the defendants and others, intercepted by means of wire tapping, amounted to a violation of the 4th and 5th Amendments.

The petitioners were convicted in the District Court for the Western District of Washington of a conspiracy to violate the National Prohibition Act by unlawfully possessing, transporting and importing intoxicating liquors and maintaining nuisances, and by selling intoxicating liquors. Seventy-two others in addition to the petitioners were indicted. Some were not apprehended, some were acquitted, and others pleaded guilty.

The evidence in the records discloses a conspiracy of amazing magnitude to import, possess and sell liquor unlawfully. It involved the employment of not less than *fifty* persons, of two seagoing vessels for the transportation of liquor to British Columbia, of smaller vessels for coastwise transportation to the state of Washington, the purchase and use of a ranch beyond the suburban limits of Seattle, with a large underground cache for storage and a number of smaller caches in that city, the maintenance of a central office manned with operators, the employment of executives, salesmen, deliverymen, dispatchers, scouts, bookkeepers, collectors and an attorney. In a bad month sales amounted to \$176,000; the aggregate for a year must have exceeded two millions of dollars.

Olmstead was the leading conspirator and the general manager of the business. He made a contribution of \$10,000 to the capital; eleven others contributed \$1,000 each. The profits were divided one-half, to Olmstead and the remainder to the other

eleven. Of the several offices in Seattle the chief one was in a large office building. In this there were three telephones on three different lines. There were telephones in an office of the manager in his own home, at the homes of his associates, and at other places in the city. Communication was had frequently with Vancouver, British Columbia. Times were fixed for the deliveries of the "stuff," to places along Puget Sound near Seattle, and from there the liquor was removed and deposited in the caches already referred to. One of the chief men was always on duty at the main office to receive orders by the telephones and to direct their filing by a corps of men stationed in another room—the "bull pen." The call numbers of the telephones were given to those known to be likely customers. At times the sales amounted to 200 cases of liquor per day.

The information which led to the discovery of the conspiracy and its nature and extent was largely obtained by intercepting messages on the telephones of the conspirators by four Federal prohibition officers. Small wires were inserted along the ordinary telephone wires from the residences of four of the petitioners and those leading from the chief office. The insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses.

The gathering of evidence continued for many months. Conversations of the conspirators, of which refreshing stenographic notes were currently made, were testified to by the government witnesses. They revealed the large business transactions of the partners and their subordinates. Men at the wires heard the orders given for liquor by customers, and the acceptances; they became auditors of the conversations between the partners. All this disclosed the conspiracy charged in the indictment. Many of the

intercepted conversations were not merely reports but parts of the criminal acts. The evidence also disclosed the difficulties to which the conspirators were subjected, the reported news of the capture of vessels, the arrest of their men and the seizure of cases of liquor in garages and other places. It showed the dealing by Olmstead, the chief conspirator, with members of the Seattle police, the messages to them which secured the release of arrested members of the conspiracy, and also direct promises to officers of payments as soon as opportunity offered.

The 4th Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." And the 5th: "No person . . . shall be compelled, in any criminal case, to be a witness against himself." . . .

There is no room in the present case for applying the 5th Amendment unless the 4th Amendment was first violated. There was no evidence of compulsion to induce the defendants to talk over their many telephones. They were continually and voluntarily transacting business without knowledge of the interception. Our consideration must be confined to the 4th Amendment....

The well-known historical purpose of the 4th Amendment, directed against general warrants and writs of assistance, was to prevent the use of governmental force to search a man's house, his person, his papers, and his effects, and to prevent their seizure against his will....

The Amendment itself shows that the search is to be of material things—the person, the house, his papers or his effects. The description of the warrant necessary to make the proceeding lawful is that it must specify the place to be searched and the person or *things* to be seized....

. . . The 4th Amendment may have proper application to a sealed letter in the mail because of the constitutional provision for the Post Office Department and the relations between the government and those who pay to secure protection of their sealed letters.... It is plainly within the words of the

Amendment to say that the unlawful rifling by a government agent of a sealed letter is a search and seizure of the sender's papers or effects. The letter is a paper, an effect, and in the custody of a government that forbids carriage except under its protection.

The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the house or offices of the defendants.

By the invention of the telephone fifty years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place.

The language of the Amendment can not be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.

This court, in *Carroll v. United States* [1925],*** declared:

The 4th Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted and in a manner which will conserve public interests as well as the interests and rights of individual citizens....

Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in Federal criminal trials, by direct legislation, and thus depart from the common law of evidence. But the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the 4th Amendment. The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the 4th Amendment. Here those who intercepted the projected voices were not in the house of either party to the conversation....

We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the 4th Amendment....

The judgments of the Circuit Court of Appeals are affirmed....

Mr. Justice Holmes: [dissenting]....

Mr. Justice Brandeis, dissenting:

... The government makes no attempt to defend the methods employed by its officers. Indeed, it concedes that if wire-tapping can be deemed a search and seizure within the 4th Amendment, such wire-tapping as was practiced in the case at bar was an unreasonable search and seizure, and that the evidence thus obtained was inadmissible. But it relies on the language of the Amendment; and it claims that the protection given thereby cannot properly be held to include a telephone conversation.

"We must never forget," said Mr. Chief Justice Marshall in *McCulloch v. Maryland*, *** "that it is a Constitution we are expounding." Since then, this court has repeatedly sustained the exercise of power by Congress, under various clauses of that instrument, over objects of which the Fathers could not have dreamed....

"... [T]ime works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosures in court of what is whispered in the closet.

Moreover, "in the applications of a constitution, our contemplation cannot be only of what has been, but of what may be." The progress of science in furnishing the government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.... Can it be that the Constitution affords no protection against such invasions of individual security?....

Time and again, this court, in giving effect to the principle underlying the 4th Amendment, has refused to place an unduly literal **construction** upon it....

The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the 4th Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the 5th.

Applying to the 4th and 5th **Amendments** the established rule of construction, the defendants' objections to the evidence obtained by a wiretapping must, in my opinion, be sustained. It is, of course, immaterial where the physical connection with the telephone wires leading into the defendants' premises was made. And it is also immaterial that the intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the government's purposes are benevolent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning, but without understanding....

Decency, security, and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen. In a government of laws, existence of the government will be imperilled if it fails to observe the law scrupulously. Our government is the potent, the omnipresent, teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the government becomes a law-breaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law the end justifies the means—to declare that the government may

commit crimes in order to secure the conviction of a private criminal—would bring terrible retribution. Against that pernicious doctrine this court should resolutely set its face.

Mr. Justice Butler, dissenting:

... This court has always construed the Constitution in the light of the principles upon which it was founded. The direct operation or literal meaning of the words used do not measure the purpose or scope of its provisions. Under the principles established and applied by this court, the 4th Amendment

safeguards against all evils that are like and equivalent to those embraced within the ordinary meaning of its words. That construction is consonant with sound reason and in full accord with the course of decisions since *McCulloch v. Maryland*. . . .

When the facts in these cases are truly estimated, a fair application of that principle decides the constitutional question in favor of the petitioners. With great deference, I think should be given a new trial.

Mr. Justice Stone, dissenting....

Privacy Policy

What is the Privacy Policy and what does it cover?

Effective January 1, 2023 | [View printable version](#) | [See previous versions](#)

We at Meta want you to understand what information we collect, and how we use and share it. That's why we encourage you to read our Privacy Policy. This helps you use Meta Products in the way that's right for you.

In the Privacy Policy, we explain how we collect, use, share, retain and transfer information. We also let you know your rights. Each section of the Policy includes helpful examples and simpler language to make our practices easier to understand. We've also added links to resources where you can learn more about the privacy topics that interest you.

It's important to us that you know how to control your privacy, so we also show you where you can manage your information in the settings of the Meta Products you use. You can [update these settings](#) to shape your experience.

Read the full policy below.

[What Products does this policy cover? >](#)

[Learn more in Privacy Center about managing your privacy >](#)

What information do we collect?



0:00 / 1:43

The information we collect and process about you depends on how you use our Products. For example, we collect different information if you sell furniture on Marketplace than if you post a reel on Instagram. When you use our Products, we collect some information about you [even if you don't have an account](#).

Here's the information we collect:

[Your activity and information you provide](#) >

[Friends, followers and other connections](#) >

[App, browser and device information](#) >

[Information from Partners, vendors and third parties](#) >

What if you don't let us collect certain information?

Some information is required for our Products to work. Other information is optional, but without it, the quality of your experience might be affected.

[Learn more >](#)

Take control in Privacy Center

 [Manage the information we collect about you](#) >

How do we use your information?

0:00 / 1:34



We use [information we collect](#) to provide a personalized experience to you, including ads, along with the other purposes we explain in detail below.

For some of these purposes, we use information [across our Products](#) and [across your devices](#). The information we use for these purposes is automatically processed by our systems. But in some cases, we also use [manual review](#) to access and review your information.

To use less information that's connected to individual users, in some cases we de-identify or aggregate information. We might also anonymize it so that it no longer identifies you. We use this information in the same ways we use your information as described in this section.

Here are the ways we use your information:

To provide, personalize and improve our Products

We use information we have to provide and improve our Products. This includes personalizing features, content and [recommendations](#), such as your [Facebook Feed](#), [Instagram feed](#), Stories and ads. We use [information with special protections](#) you choose to provide for these purposes, but not to show you ads.

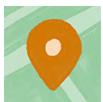
Read more about how we use information to provide, personalize and improve our Products:



[How we show ads and other sponsored or commercial content](#) >



[How we use information to improve our Products](#) >



How we use location-related information >

To promote safety, security and integrity

We use information we collect to help protect people from harm and provide safe, secure Products.

[Learn more >](#)

To provide measurement, analytics and business services

Lots of people rely on our Products to run or promote their businesses. We help them measure how well their ads and other content are working.

[Learn more >](#)

To communicate with you

We communicate with you using information you've given us, like contact information you've entered on your profile.

[Learn more >](#)

To research and innovate for social good

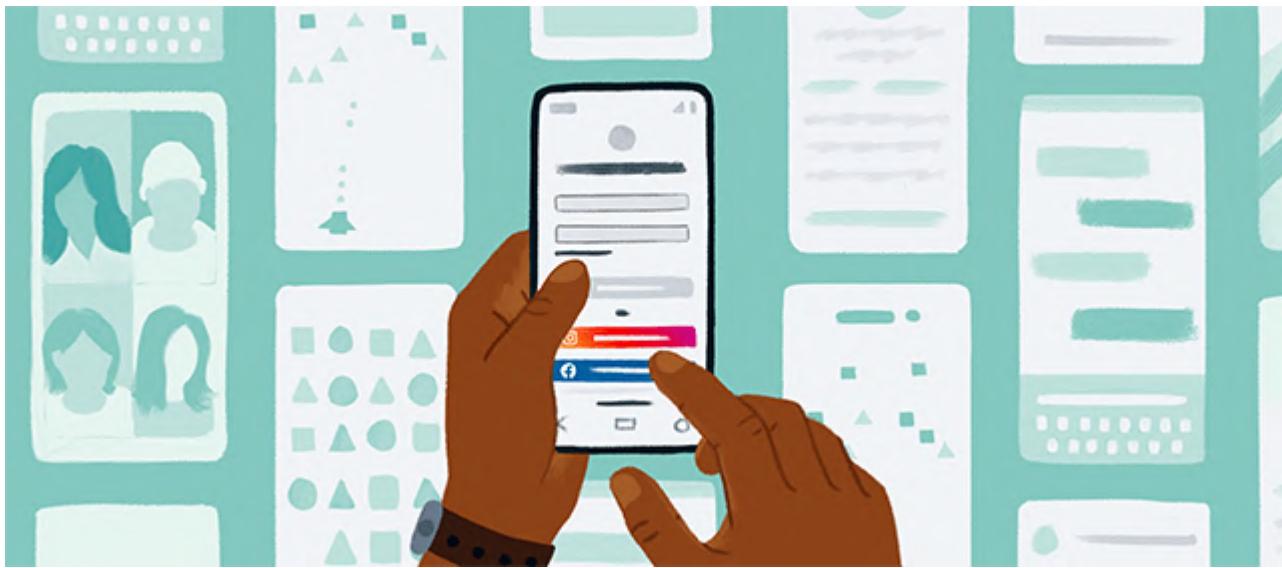
We use information we have, information from researchers and datasets from publicly available sources, professional groups and non-profit groups to conduct and support research.

[Learn more >](#)

More in the Privacy Policy

Why and how we process your information >

How is your information shared on Meta Products or with Integrated Partners?



On Meta Products

Learn more about the different cases when your information can be shared on our Products:

[People and accounts you share and communicate with](#) >

[Content others share or reshare about you](#) >

[Public content](#) >

With Integrated Partners

You can choose to connect with [Integrated Partners](#) who use our Products. If you do, these Integrated Partners receive information about you and your activity.

These Integrated Partners can always access information that's public on our Products. Learn more about other information they receive and how they handle your information:

[When you use an Integrated Partner's product or service](#) >

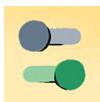
[When you interact with someone else's content on an Integrated Partner's product or service](#) >

[How Integrated Partners handle your information](#) >

Take control

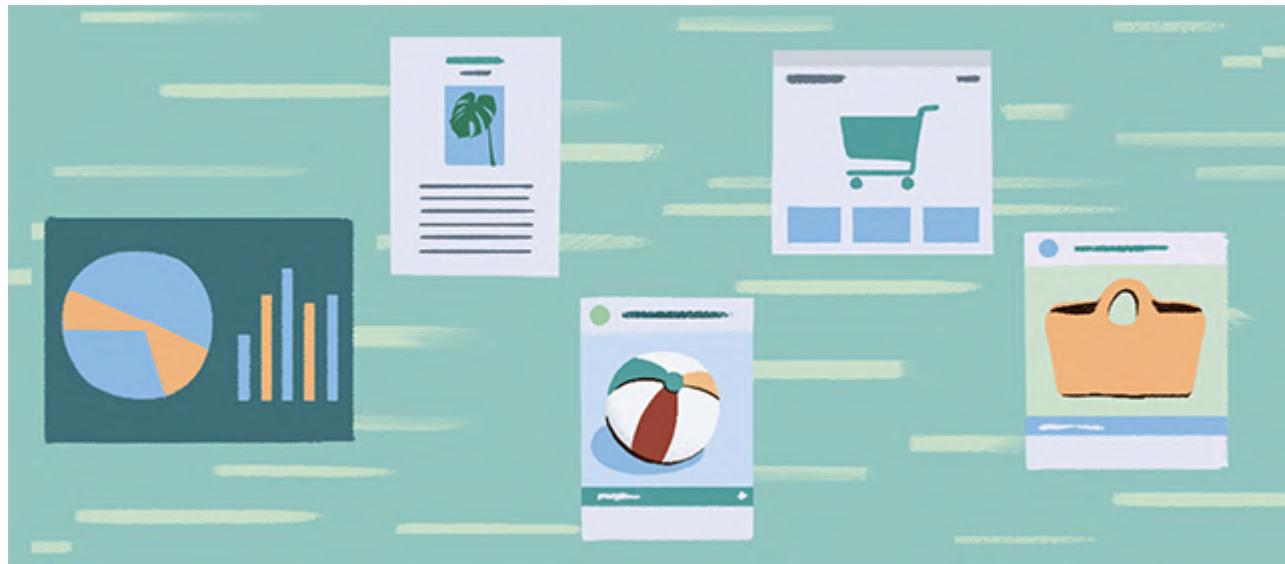


[Learn more about audiences in Privacy Center](#) >



Manage apps and websites >

How do we share information with Partners, vendors, service providers and third parties?



We don't sell any of your information to anyone, and we never will. We also require Partners and third parties to follow rules about how they can and cannot use and disclose the information we provide.

Here's more detail about who we share information with:

Partners

[Advertisers and Audience Network publishers](#) >

[Partners who use our analytics services](#) >

[Partners who offer goods or services on our Products and commerce services platforms](#) >

[Integrated Partners](#) >

Vendors

[Measurement and marketing vendors](#) >

Service providers

Service providers >

Third parties

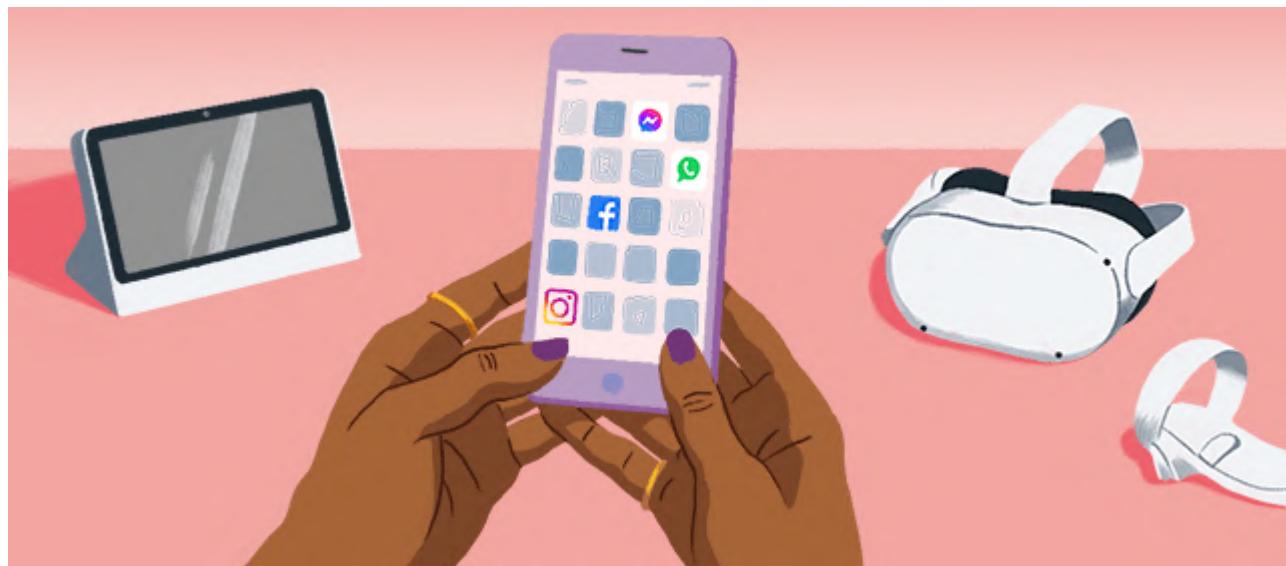
External researchers >

Other times we share with third parties

We also share information with third parties in response to legal requests, to comply with applicable law or to prevent harm. [Read the policy](#).

And if we sell or transfer all or part of our business to someone else, then we may give the new owner your information as part of that transaction, in line with applicable law.

How do the Meta Companies work together?



We are part of the [Meta Companies](#) that provide Meta Company Products.

[Meta Company Products](#) include all the Meta Products covered by this Policy, plus other products like WhatsApp, Novi and more.

We share information we collect, infrastructure, systems and technology with the other Meta Companies. [Learn more](#) about how we transfer information to other countries.

We also process information that we receive about you from other Meta Companies, according to their terms and policies and as permitted by applicable law. In some cases, Meta acts as a service provider for other Meta Companies. We act on their behalf and in accordance with their instructions and terms.

Why we share across the Meta Companies

Meta Products share information with other Meta Companies:

- To promote safety, security and integrity and comply with applicable laws
- To personalize offers, ads and other sponsored or commercial content

- To develop and provide features and integrations
- To understand how people use and interact with Meta Company Products

[See some examples](#) of why we share.

More resources

Review the privacy policies of the other Meta Companies

[Facebook Help Center](#)

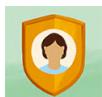


How can you manage or delete your information and exercise your rights?

We offer you a variety of tools to view, manage, download and delete your information below. You can also manage your information by visiting the settings of the Products you use. You may also have other privacy rights under applicable laws.

To exercise your rights, visit our Help Centers, your settings for Facebook and Instagram and your device-based settings.

Take a privacy checkup



Take a privacy checkup

Be guided through Facebook privacy settings



View and manage your information

Access your information >

Off-Facebook activity >

Ad preferences >

Manage your data

Port, download or delete your information

Port your information >

Download your information >



Delete your information or account



You can learn more about how privacy works on [Facebook](#) and on [Instagram](#), and in the [Facebook Help Center](#). If you have questions about this policy, you can [contact us](#) as described below. In some countries, you may also be able to contact the Data Protection Officer for Meta Platforms, Inc., and depending on your jurisdiction, you may also contact your local Data Protection Authority ("DPA") directly.

How long do we keep your information?

We keep information as long as we need it to provide our Products, comply with legal obligations or protect our or other's interests. We decide how long we need information on a case-by-case basis. Here's what we consider when we decide:

- If we need it to operate or provide our Products. For example, we need to keep some of your information to maintain your account. [Learn more](#).
- The feature we use it for, and how that feature works. For example, messages sent using Messenger's vanish mode are retained for less time than regular messages. [Learn more](#).
- How long we need to retain the information to comply with certain legal obligations. [See some examples](#).
- If we need it for other legitimate purposes, such as to prevent harm; investigate possible violations of our terms or policies; promote safety, security and integrity; or protect ourselves, including our rights, property or products

In some instances and for specific reasons, we'll keep information for an extended period of time. [Read our policy](#) about when we may preserve your information.

How do we transfer information?

Why is information transferred to other countries? >

Where is information transferred? >

How do we safeguard your information? >

How do we respond to legal requests, comply with applicable law and prevent harm?

We access, preserve, use and share your information:

- In response to legal requests, like search warrants, court orders, production orders or subpoenas. These requests come from third parties such as civil litigants, law enforcement and other government authorities. [Learn more](#) about when we respond to legal requests.
- In accordance with applicable law

- To promote the safety, security and integrity of Meta Products, users, employees, property and the public. [Learn more](#).

We may access or preserve your information for an extended amount of time. [Learn more](#).

How will you know the policy has changed?

We'll notify you before we make material changes to this Policy. You'll have the opportunity to review the revised Policy before you choose to continue using our Products.

Privacy notice for United States residents

You can learn more about the consumer privacy rights that may be available to you by reviewing the [United States Regional Privacy Notice](#).

How to contact Meta with questions

You can learn more about how privacy works on [Facebook](#) and on [Instagram](#) and in the [Facebook Help Center](#). If you have questions about this Policy or have questions, complaints or requests regarding your information, you can contact us as described below.

You can contact us [online](#) or by mail at:

Meta Platforms, Inc.

ATTN: Privacy Operations

1601 Willow Road

Menlo Park, CA 94025

Why and how we process your information

The categories of information we use, and why and how information is processed, are set out below:

Why and how we process your information	Information categories we use (see ' What Information do we collect? ' for more information on each information category) The actual information we use depends on your factual circumstances, but could include any of the following:
Personalizing the Meta Products: Our systems automatically process information we collect and store associated with you and others to assess and understand your interests and your preferences and provide you personalized	Your activity and information you provide: <ul style="list-style-type: none">• Content you create, like posts, comments or audio

Why and how we process your information	Information categories we use (see ' What Information do we collect? ' for more information on each information category)
<p>experiences across the Meta Products in accordance with our terms. This is how we:</p> <ul style="list-style-type: none"> • Personalize features and content (such as your News Feed, Instagram Feed and Stories); • Personalize the ads people see; and • Make suggestions for you (such as people you may know, groups or events that you may be interested in or topics that you may want to follow) on and off our products. <p>Learn more about how we use information about you to personalize your experience on and across Meta Products and how we choose the ads that you see.</p>	<p>The actual information we use depends on your factual circumstances, but could include any of the following:</p> <ul style="list-style-type: none"> • Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features • Metadata about content • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them • Purchases or other transactions you make • Hashtags you use • The time, frequency and duration of your activities on our Products <p>Friends, followers and other connections</p> <p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device characteristics and device software • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your device apart from other users' • Device signals • Information you've shared through your device settings (like GPS location) • Information about the network you connect your device to • Reports about our products' performance on your device

<p>Why and how we process your information</p>	<p>Information categories we use (see 'What Information do we collect?' for more information on each information category)</p> <p>The actual information we use depends on your factual circumstances, but could include any of the following:</p>
	<ul style="list-style-type: none"> Information from cookies and similar technologies <p>Information from Partners, vendors and third parties. (You have control over Meta's use of Partner data to tailor ads to you.)</p>
<p>Providing and improving our Meta Products: The provision of the Meta Products includes collecting, storing, and, where relevant, sharing, profiling, reviewing and curating, and in some instances not only automated processing but also manual (human) reviewing, to:</p> <ul style="list-style-type: none"> Create and maintain your account and profile, Facilitate the sharing of content and status, Provide and curate features, Provide messaging services, the ability to make voice and video calls and connect with others, Provide advertising products, and Undertake analytics. <p>We also use information to develop, research and test improvements to our Products. We use information we have to:</p> <ul style="list-style-type: none"> See if a product is working correctly, Troubleshoot and fix it when it's not, Test out new products and features to see if they work, Get feedback on our ideas for products or features, and Conduct surveys and other research about what you like about our Products and brands and what we can do better. 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> Content you create, like posts, comments or audio Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features Messages you send and receive, including their content, subject to applicable law Metadata about content and messages, subject to applicable law Types of content you view or interact with, and how you interact with it Apps and features you use, and what actions you take in them Purchases or other transactions you make, including truncated credit card information Hashtags you use The time, frequency and duration of your activities on our Products <p>Friends, followers and other connections</p> <p>App, browser and device information:</p> <ul style="list-style-type: none"> Device characteristics and device software

<p>Why and how we process your information</p>	<p>Information categories we use (see 'What Information do we collect?' for more information on each information category)</p> <p>The actual information we use depends on your factual circumstances, but could include any of the following:</p>
	<ul style="list-style-type: none"> • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your device apart from other users' • Device signals • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies <p>Information from Partners, vendors and third parties</p>
<p>Promoting safety, integrity and security on and across the Meta Products: The Meta Products are designed to research and help ensure the safety, integrity and security of those services and those people who enjoy them, on and off Meta Products. We process information we have associated with you and apply automated processing techniques and, in some instances, conduct manual (human) review to:</p> <ul style="list-style-type: none"> • Verify accounts and activity, • Find and address violations of our terms or policies. In some cases, the decisions we make about violations are reviewed by the Oversight Board, • Investigate suspicious activity, • Detect, prevent and combat harmful or unlawful behavior, such as to review and, in some cases, remove content reported to us, 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Content you create, like posts, comments or audio • Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features • Messages you send and receive, including their content, subject to applicable law • Metadata about content and messages, subject to applicable law • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them

<h2>Why and how we process your information</h2>	<p>Information categories we use (see 'What Information do we collect?' for more information on each information category)</p> <p>The actual information we use depends on your factual circumstances, but could include any of the following:</p>
<ul style="list-style-type: none"> Identify and combat disparities and racial bias against historically marginalized communities, Protect the life, physical or mental health, well-being or integrity of our users or others, Detect and prevent spam, other security matters and other bad experiences, Detect and stop threats to our personnel and property, and Maintain the integrity of our Products. <p>For more information on safety, integrity and security generally on Meta Products, visit the Facebook Security Help Center and Instagram Security Tips.</p>	<ul style="list-style-type: none"> Purchases or other transactions you make, including truncated credit card information Hashtags you use The time, frequency and duration of your activities on our Products Friends, followers and other connections <p>App, browser and device information:</p> <ul style="list-style-type: none"> Device characteristics and device software What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) Identifiers that tell your device apart from other users' Device signals Information you've shared through your device settings Information about the network you connect your device to, including your IP address Information from cookies and similar technologies <p>Information from Partners, vendors and third parties</p>
<p>To communicate with you: We use information you've given us (like contact information on your profile) to send you a communication, like an e-mail or in-product notice, for example:</p> <ul style="list-style-type: none"> We'll contact you via email or in-product notifications in relation to the Meta Products, 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> Contact information on your profile and your communications with us Content you create, like posts, comments or audio

Why and how we process your information	Information categories we use (see 'What Information do we collect?' for more information on each information category) The actual information we use depends on your factual circumstances, but could include any of the following:
<p>product-related issues, research or to let you know about our terms and policies. We also use contact information like your email address to respond when you contact us.</p>	<ul style="list-style-type: none"> Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features <p>App, browser and device information:</p> <ul style="list-style-type: none"> Device characteristics and device software What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) Identifiers that tell your device apart from other users' Device signals Information you've shared through your device settings Information about the network you connect your device to, including your IP address Information from cookies and similar technologies.
<p>Transferring, storing or processing your information across borders, including from and to the United States and other countries: We share information we collect globally, both internally across our offices and data centers and externally with our Partners, third parties and service providers. Because Meta is global, with users, Partners, vendors and employees around the world, transfers are necessary:</p> <ul style="list-style-type: none"> To operate and provide the services described in the terms that apply to the Meta Product(s) you are using. This includes 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> Content you create, like posts, comments or audio Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features Metadata about content and messages, subject to applicable law

Why and how we process your information	Information categories we use (see 'What Information do we collect?' for more information on each information category) The actual information we use depends on your factual circumstances, but could include any of the following:
<p>allowing you to share information and connect with your family and friends around the globe; and</p> <ul style="list-style-type: none"> • To fix, analyze and improve our Products. For more information, see the "How do we transfer information?" section of the Meta Privacy Policy. 	<ul style="list-style-type: none"> • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them • Purchases or other transactions you make, including truncated credit card information • Hashtags you use • The time, frequency and duration of your activities on our Products Friends, followers and other connections <p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device characteristics and device software • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your advice apart from other users' • Device signals • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies <p>Information from Partners, vendors and third parties</p>
Processing information subject to special protections under applicable laws that you provide so we can share it with those you	<p>Your activity and information you provide:</p>

Why and how we process your information	Information categories we use (see 'What Information do we collect?' for more information on each information category) The actual information we use depends on your factual circumstances, but could include any of the following:
choose, to provide, personalize and improve our Products and to undertake analytics. We'll collect, store, publish and apply automated, or sometimes manual (human), processing for these purposes.	<ul style="list-style-type: none"> • Any information with special protections that you choose to provide in your profile fields (such as your religious views, political views, or who you are "interested in"), or as part of surveys you choose to participate in
Receiving and using information from third parties to tailor the ads you see: We'll use information that advertisers, businesses and other partners provide us about activity off Meta Products that we have associated with you to personalize ads that we show you on Meta Products, and on websites, apps and devices that use our advertising services. We receive this information whether or not you're logged in or have an account on our Products. See the Cookies Policy for more information.	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Information and content you provide, such as your name or email address <p>Information from Partners, vendors and third parties</p>
Sharing your contact, profile or other information with third parties upon your request: The type of third party and categories of information shared depend on the circumstances of what you ask us to share. For example: <ul style="list-style-type: none"> • We share your email (or other contact information) or other information you might choose when you direct us to share it with an advertiser so they can contact you with additional information about a promoted product, and • If you choose to integrate other apps, games or websites with Meta Products and log in, we'll share your information with the app, game or website to log you in. 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Content you create, like your contact, profile or other information, like posts or comments

Why and how we process your information	Information categories we use (see 'What Information do we collect?' for more information on each information category) The actual information we use depends on your factual circumstances, but could include any of the following:
<p>Providing measurement, analytics and business services: Our systems automatically, as well as with some manual (human) processing, process information we have collected and stored about you and others. We use this information to:</p> <ul style="list-style-type: none"> • Provide insights and measurement reports to businesses, advertisers and other Partners to help them measure the effectiveness and distribution of their or their clients' ads, content and services, to understand the kinds of people who are seeing their content and ads, and how their content and ads are performing on and off Meta Products, and • Provide aggregated user analytics and insights reports that help businesses, advertisers and other Partners better understand the audiences with whom they may want to connect, as well as the types of people who use their services and how people interact with their websites, apps and services. 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Content you create, like posts, comments or audio • Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them • Purchases or other transactions you make • Hashtags you use • The time, frequency and duration of your activities on our Products <p>Friends, followers and other connections</p> <p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device characteristics and device software • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your device apart from other users • Device signals • Information you've shared through your device settings • Information about the network you connect your device to, including your

<p>Why and how we process your information</p>	<p>Information categories we use (see 'What Information do we collect?' for more information on each information category)</p> <p>The actual information we use depends on your factual circumstances, but could include any of the following:</p>
	<ul style="list-style-type: none"> IP address • Information from cookies and similar technologies
<p>Sharing of information across the Meta Companies:</p> <ul style="list-style-type: none"> • To provide a seamless, consistent and richer, innovative experience across the Meta Company Products to enable cross app interactions, sharing, viewing and engaging with content, including posts and videos. 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Content you create, like posts, comments or audio • Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features • Metadata about content • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them • Purchases or other transactions you make • Hashtags you use • The time, frequency and duration of your activities on our Products <p>Friends, followers and other connections</p> <p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device characteristics and device software • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your device apart from other users' • Device signals

<p>Why and how we process your information</p>	<p>Information categories we use (see 'What Information do we collect?' for more information on each information category)</p> <p>The actual information we use depends on your factual circumstances, but could include any of the following:</p>
	<ul style="list-style-type: none"> • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies
<p>Business intelligence and analytics:</p> <ul style="list-style-type: none"> • To understand, in aggregate, your usage of and across our Products, to accurately count people and businesses; and • To validate metrics directly related to these, in order to inform and improve product direction and development and to adhere to (shareholder/earning) reporting obligations. 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Content you create, like posts, comments or audio • Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features • Metadata about content and messages, subject to applicable law • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them • Purchases or other transactions you make • Hashtags you use • The time, frequency and duration of your activities on our Products <p>Friends, followers and other connections</p> <p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device characteristics and device software

<p>Why and how we process your information</p>	<p>Information categories we use (see 'What Information do we collect?' for more information on each information category)</p> <p>The actual information we use depends on your factual circumstances, but could include any of the following:</p>
	<ul style="list-style-type: none"> • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your device apart from other users' • Device signals • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies <p>Information from Partners, vendors and third parties</p>
<p>Identifying you as a Meta Product user and personalizing the ads we show you through Meta Audience Network when you visit other apps:</p> <ul style="list-style-type: none"> • When we show you ads through Meta Audience Network when you visit other apps, our systems automatically process the information we have collected and stored about you and others to identify you as a Meta Product user and tailor the ads you see. 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Information you provide • Content you create, like posts, comments or audio • Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features • Metadata about content • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them • Purchases or other transactions you make • Hashtags you use

<p>Why and how we process your information</p>	<p>Information categories we use (see 'What Information do we collect?' for more information on each information category)</p> <p>The actual information we use depends on your factual circumstances, but could include any of the following:</p>
	<ul style="list-style-type: none"> • The time, frequency and duration of your activities on our Products Friends, followers and other connections <p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device characteristics and device software • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your device apart from other users' • Device signals • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies
<p>Providing marketing communications to you:</p> <ul style="list-style-type: none"> • Depending on your settings and subject to applicable law, we'll share marketing communications with you. • We'll collect and store your information and use it to send marketing communications to you, like an email, subject to applicable laws. 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Information and content you provide, including your contact information like email address <p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device identifiers
<p>Research and innovate for social good:</p> <ul style="list-style-type: none"> • We carry out surveys and use information (including from researchers we collaborate 	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Content you create, like posts, comments or audio

Why and how we process your information	Information categories we use (see ' What Information do we collect? ' for more information on each information category)
<p>with) to conduct and support research and innovation on topics of general social welfare, technological advancement, public interest, health and well-being.</p> <ul style="list-style-type: none"> For example, we analyze information that we have about migration patterns during crises. This helps relief organizations get aid to the right places. We collect, store, combine, analyze and apply automatic processing techniques like aggregation of information as well as manual (human) review, and share information, as necessary to research and innovate for social good in this way. We do this to do things like create COVID-19 forecasting models. <p>Learn more  about our research programs.</p>	<p>The actual information we use depends on your factual circumstances, but could include any of the following:</p> <ul style="list-style-type: none"> Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features Metadata about content and messages, subject to applicable law Types of content you view or interact with, and how you interact with it Apps and features you use, and what actions you take in them Purchases or other transactions you make Hashtags you use The time, frequency and duration of your activities on our Products Friends, followers and other connections <p>App, browser and device information:</p> <ul style="list-style-type: none"> Device characteristics and device software What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) Identifiers that tell your device apart from other users' Device signals Information you've shared through your device settings Information about the network you connect your device to, including your IP address Information from cookies and similar technologies

<p>Why and how we process your information</p>	<p>Information categories we use (see 'What Information do we collect?' for more information on each information category)</p> <p>The actual information we use depends on your factual circumstances, but could include any of the following:</p>
	<p>Information from Partners, vendors and third parties</p>
<p>Anonymizing your information In some cases, we anonymize information we have associated with you, such as your activity on and off our Products, and use the resulting information, for example, to provide and improve our Meta Products, including ads.</p>	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Content you create, like posts, comments or audio • Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features • Metadata about content • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them • Purchases or other transactions you make • Hashtags you use • The time, frequency and duration of your activities on our Products <p>Friends, followers and other connections</p> <p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device characteristics and device software • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your device apart from other users' • Device signals

<p>Why and how we process your information</p>	<p>Information categories we use (see 'What Information do we collect?' for more information on each information category)</p> <p>The actual information we use depends on your factual circumstances, but could include any of the following:</p>
	<ul style="list-style-type: none"> • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies <p>Information from Partners, vendors and third parties</p>
<p>Share information with others, including law enforcement and to respond to legal requests. See the "How do we respond to legal requests, prevent harm and promote safety and integrity?" section of the Meta Privacy Policy for more for information on when we share information with law enforcement and others.</p> <p>The categories of information we access, preserve, use and share depend on the specific circumstances. For example, responses to legal requests where not compelled by law will typically include limited information (such as contact details and login information). However, the information we process will depend on the purposes, which could include the following:</p> <ul style="list-style-type: none"> • In response to legal requests from third parties such as civil litigants, law enforcement and other government authorities • To comply with applicable law or legitimate legal purposes • To promote the safety, security and integrity of Meta Companies, Meta Products, users, employees, property and the public <p>Learn more about how we promote safety, security and integrity.</p>	<p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Content you create, like posts, comments or audio • Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features • Metadata about content, subject to applicable law • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them • Purchases or other transactions you make • Hashtags you use <p>Friends, followers and other connections</p> <p>app, browser and device information:</p> <ul style="list-style-type: none"> • Device characteristics and device software • What you're doing on your device (like whether our app is in the

<p>Why and how we process your information</p>	<p>Information categories we use (see 'What Information do we collect?' for more information on each information category)</p> <p>The actual information we use depends on your factual circumstances, but could include any of the following:</p>
	<p>foreground or if your mouse is moving)</p> <ul style="list-style-type: none"> • Identifiers that tell your device apart from other users' • Device signals • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies <p>Information from Partners, vendors and third parties</p>
<p>For processing information when the law requires it: Where we are under an obligation to disclose information such as, for example, if we receive a valid legal request for certain information such as a search warrant, we will access, preserve and/or share your information with regulators, law enforcement or others. The way in which the information will be processed depends on the specific circumstances. See the "How do we respond to legal requests, prevent harm and promote safety and integrity?" section of the Meta Privacy Policy for more.</p> <p>Information for Law Enforcement Authorities ↗ provides information on the operational guidelines law enforcement needs to follow.</p>	<p>The categories of information depend on the specific circumstances of each mandatory request or obligation. Only the information necessary to comply with the relevant legal obligation will be shared or otherwise processed. For example, for civil matters, this will typically include limited information (such as contact details and login information). However, depending on the circumstances it could include the following:</p> <p>Your activity and information you provide:</p> <ul style="list-style-type: none"> • Content you create, like posts, comments or audio • Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features • Messages you send and receive, including their content, subject to

<p>Why and how we process your information</p>	<p>Information categories we use (see 'What Information do we collect?' for more information on each information category)</p> <p>The actual information we use depends on your factual circumstances, but could include any of the following:</p>
	<p>applicable law</p> <ul style="list-style-type: none"> • Metadata about content and messages, subject to applicable law • Types of content you view or interact with, and how you interact with it • Apps and features you use, and what actions you take in them • Purchases or other transactions you make, including truncated credit card information • Hashtags you use • The time, frequency and duration of your activities on our Products Friends, followers and other connections <p>App, browser and device information:</p> <ul style="list-style-type: none"> • Device characteristics and device software • What you're doing on your device (like whether our app is in the foreground or if your mouse is moving) • Identifiers that tell your device apart from other users' • Device signals • Information you've shared through your device settings • Information about the network you connect your device to, including your IP address • Information from cookies and similar technologies

Why and how we process your information	<p>Information categories we use (see 'What Information do we collect?' for more information on each information category)</p> <p>The actual information we use depends on your factual circumstances, but could include any of the following:</p>
	<p>Information from Partners, vendors and third parties</p>

[Log in or sign up](#)[Home](#) > [Privacy Policy](#)[Legal terms](#)

Privacy Policy



For a list of Privacy Policies by jurisdiction, click [here](#).

Last Updated: January 25, 2023

Airbnb exists to help build connections between people and make the world more open and inclusive. In short—to build a world where anyone can belong anywhere. We are a community built on trust. A fundamental part of earning that trust means being clear about how we use your information and protecting your human right to privacy.

This Privacy Policy describes how Airbnb, Inc. and its affiliates (“**we**,” “**us**,” or “**Airbnb**”), process personal information in relation to your use of the Airbnb Platform. Depending on where you live and what you are doing on the Airbnb Platform, the supplemental privacy pages listed below may apply to you. Please follow the links and review the supplemental information describing how we process personal information for those regions and services.



IMPORTANT SUPPLEMENTAL INFORMATION

Outside of the United States. If you reside outside of the United States, such as in the European Economic Area (“EEA”) visit our “[Outside of the United States](#)” page to learn about (i) the controller(s) of your personal information, (ii) legal bases, including legitimate interests, for collecting and processing your personal information, (iii) safeguards relied upon for transferring personal information outside the EEA, (iv) your rights, and (v) contact details of the controller(s) and Data Protection Officer.

- If you are resident in the EEA and Switzerland, Airbnb Payments Luxembourg SA, 4 rue Henri Schnadt, L-2350 Luxembourg, is the controller of your personal information in relation to Payment Services.
- Airbnb Payments UK Limited, 100 New Bridge Street, London, EC4V 6JA, United Kingdom, is the controller of your personal information if you are resident in (a) Australia, for all Payment Services except for those in connection with booking any Host Service; (b) China, for Payments Services in connection with: (i) booking or offering any Host Service, located outside your country of residence, or (ii) booking a Host Service located in your country of residence where the Host resides outside your country of residence); (c) Brazil, for Payments Services in connection with: (i) booking a Host Service, located outside of Brazil, where the Host resides outside of Brazil and paying in foreign currency, or (ii) offering any Host Service, located outside Brazil, where the Guest booking the service resides outside of Brazil and pays in foreign currency* (d) India, for Payments Services in connection with (i) booking or offering any Host Service, located outside India, or (ii) offering a Host Service in India to a Guest who resides outside of India; or (e) Japan and all other countries other than the EEA, Switzerland and United States, for Payment Services for all activities.
- If you are resident in Australia, UK, the EEA and Switzerland, India, Brazil*, and all other countries outside of the United States except China and Japan, Airbnb Ireland UC, 8 Hanover Quay, Dublin 2, Ireland, is the controller of your personal information in relation to all activities other than Payment Services.
- If you reside in China, Airbnb Ireland UC is the controller of your personal information in relation to booking or offering any Host Service located outside China.
- If you reside in Japan, Airbnb Ireland UC is the controller of your personal information in relation to booking or offering any Host Service located outside Japan and Airbnb Global Services Limited is the controller for all other activities except for Payment Services.
- *If you reside in Brazil, Airbnb Plataforma Digital Ltda is the controller of your personal information in relation to all activities, including Payment Services, from April 1, 2022.
- To contact the Data Protection Officer (DPO) for Airbnb Ireland or the Brazil Data Protection Officer (Brazil DPO) for Airbnb Plataforma Digital Ltda, click [here](#).

China. If you reside in the People's Republic of China, which for purposes of this Privacy Policy does not include Hong Kong, Macau and Taiwan ("China"), visit our "[China](#)" page to learn more about Airbnb Internet (Beijing) Co. Ltd. (安彼迎网络 (北京) 有限公司) ("Airbnb China") and how your information is handled in relation to activities within China and your rights.

Enterprise Customers and Airbnb for Work. If you use our enterprise services or have linked your account with an Airbnb for Work customer, visit our "[Enterprise Customers and Airbnb for Work](#)" page to learn about specific privacy information that applies to you.

1. DEFINITIONS

Undefined terms in this Privacy Policy have the same definition as in our [Terms of Service](#) (“**Terms**

2. PERSONAL INFORMATION WE COLLECT

2.1 Information Needed to Use the Airbnb Platform.

We collect personal information about you when you use the Airbnb Platform. Without it, we may not be able to provide all services requested. This information includes:

- **Contact, Account, and Profile Information.** Such as your first name, last name, phone number, postal address, email address, date of birth, and profile photo, some of which will depend on the features you use.
- **Identity Verification and Payment Information.** Such as images of your government-issued ID (as permitted by applicable laws), your ID number or other verification information, a selfie when we verify your ID, bank account or payment account information. If you are not an Airbnb user, we may receive payment information relating to you, such as when an Airbnb user provides your payment card to complete a booking. If a copy of your ID is provided to us, we may scan, use, and store information contained in your ID to verify your identity and for security purposes.

2.2 Information You Choose to Give Us.

You can choose to provide us with additional personal information. This information may include:

- **Additional Profile Information.** Such as gender, preferred language(s), city, and personal description. Some of this information as indicated in your account settings is part of your public profile page and will be publicly visible.
- **Information About Others.** Such as a payment instrument belonging to another person or information about a co-traveler. By providing us with personal information about others, you certify that you have permission to provide that information to Airbnb for the purposes described in this Privacy Policy and you have shared the Airbnb Privacy Policy with them.
- **Other Information.** Such as when you fill in a form, add information to your account, respond to surveys, post to community forums, participate in promotions, communicate with Airbnb Support and other Members, import or manually enter address book contacts, provide your address and/or geolocation,

or share your experience with us. This may include health information if you choose to share it with us.

2.3 Information Automatically Collected by Using the Airbnb Platform and Our Payment Services.

When you use the Airbnb Platform and Payment Services, we automatically collect personal and other information. This information may include:

- **Geolocation Information.** Such as precise or approximate location determined from your IP address, mobile or other device's GPS, or other information you share with us, depending on your device settings. We may also collect this information when you're not using the app if you enable this through your settings or device permissions.
- **Usage Information.** Such as the pages or content you view, searches for Listings, bookings you have made, additional services you have added, and other actions on the Airbnb Platform.
- **Log Data and Device Information.** Such as details about how you've used the Airbnb Platform (including if you clicked on links to third-party applications), IP address, access dates and times, hardware and software information, device information, device event information, unique identifiers, crash data, and the pages you've viewed or engaged with before or after using the Airbnb Platform. We may collect this information even if you haven't created an Airbnb account or logged in.
- **Cookies and Similar Technologies As Described in Our Cookie Policy.**
- **Payment Transaction Information.** Such as payment instrument used, date and time, payment amount, payment instrument expiration date and billing postcode, PayPal email address, IBAN information, your address, and other related transaction details.

2.4 Personal Information We Collect from Third Parties.

We collect personal information from other sources, such as:

- **Third-Party Services.** If you link, connect, or login to the Airbnb Platform with a third-party service (e.g., Google, Facebook, WeChat), you direct the service to send us information such as your registration, friends list, and profile information as controlled by that service or as authorized by you via your privacy settings at that service.

- **Background Information.** For Members in the United States, to the extent permitted by applicable laws, we may obtain, for example, reports of criminal records, sex offender registrations, and other information about you and/or your background. For Hosts in India, to the extent permitted by applicable laws, we may perform criminal background checks. For Members outside of the United States, to the extent permitted by applicable laws and with your consent where required, we may obtain police, background, or registered sex offender checks. We may use your information, including your full name and date of birth, to obtain such reports.
- **Enterprise Product Invitations and Account Management.** Organizations that use our Enterprise products may submit personal information to facilitate account management and invitations to use enterprise products.
- **Referrals and Co-Travelers.** If you are invited to the Airbnb Platform, for example, as a co-traveler on a trip, the person who invited you can submit personal information about you such as your email address or other contact information.
- **Guest Travel Insurance.** If you make a claim under our Guest Travel Insurance policy, we will receive information regarding your claim in order to process, handle, or assess your claim and as outlined in this Privacy Policy.
- **Other Sources.** To the extent permitted by applicable law, we may receive additional information about you, such as references, demographic data, or information to help detect fraud and safety issues from third-party service providers and/or partners, and combine it with information we have about you. For example, we may receive background check results or fraud warnings from identity verification service providers for use in our fraud prevention, security investigation, and risk assessment efforts. We may receive information about you and your activities on and off the Airbnb Platform, or about your experiences and interactions from our partners. We may receive health information, including but not limited to, health information related to contagious diseases.

3. HOW WE USE INFORMATION WE COLLECT



If you reside outside of the United States, click [here](#) to learn about our legal bases for collection and processing personal information. We use personal information as outlined in this Privacy Policy.

3.1 Provide, Improve, and Develop the Airbnb Platform. We may process this information to:

- enable you to access the Airbnb Platform and make and receive payments,
- enable you to communicate with other Members,
- process your request,
- perform analytics, debug, and conduct research,
- provide customer service training,
- send you messages, updates, security alerts, and account notifications,
- process, handle, or assess insurance claims or similar claims,
- personalize and customize your experience based on your interactions with the Airbnb Platform, your search and booking history, your profile information and preferences, and other content you submit, and
- enable your use of our enterprise products and accommodation services.

If you provide us with your contacts' information, such as your friends or co-travelers, we may process this information to: (i) facilitate your referral invitations, (ii) share your trip details and facilitate trip planning, (iii) detect and prevent fraud, and (iv) facilitate your requests or for any other purpose you authorize.

3.2 Create and Maintain a Trusted and Safer Environment. We may process this information to:

- detect and prevent fraud, spam, abuse, security and safety incidents, and other harmful activities,
- study and combat discrimination consistent with our [Nondiscrimination Policy](#),
- conduct fraud prevention, security investigations, and risk assessments,
- verify or authenticate information provided by you,
- conduct checks against databases and other information sources, including background checks,
- comply with our legal obligations, protect the health and well-being of our Guests, Hosts, Hosts' employees, and members of the public,

- resolve disputes with our Members, including sharing information with your co-Host(s) or additional Guests about disputes related to your role as a co-Host(s) or additional Guests,
- enforce our agreements with third parties,
- determine eligibility for certain types of bookings, such as Instant Book,
- comply with law, respond to legal requests, prevent harm, and protect our rights (see section 4.5),
- enforce our Terms and other policies (e.g., Nondiscrimination Policy), and
- assess or evaluate your interactions with the Airbnb Platform and information obtained from third parties. In limited cases, automated processes, which analyze your account and activities on the Airbnb platform as well as information in relation to activities on and off the Airbnb platform that can be associated with you, could restrict or suspend your access to the Airbnb Platform if such processes detect activity that may pose a safety or other risk to Airbnb, our community, or third parties. If you would like to challenge decisions based on automated processes, please contact us via the Contact Information section below. You can find out more about how our system determines whether certain reservations may carry a higher risk for incidents here.

3.3 Provide, Personalize, Measure, and Improve our Advertising and Marketing. We may process this information to:

- send you promotional messages, marketing, advertising, and other information based on your preferences and social media advertising through social media platforms,
- personalize, measure, and improve our advertising,
- administer referral programs, rewards, surveys, sweepstakes, contests, or other promotional activities or events sponsored or managed by Airbnb or its third-party partners,
- analyze characteristics and preferences to send you promotional messages, marketing, advertising, and other information that we think might be of interest to you,
- invite you to events and relevant opportunities, and

- send, with your consent, promotional messages, marketing, advertising, and other information that may be of interest to you based on your preferences.

3.4 Analyzing and Sharing Your Communications.

We may review, scan, or analyze your communications on the Airbnb Platform for reasons outlined in the “How We Use Information We Collect” section of this policy, including fraud prevention, security investigations, risk assessment, regulatory compliance, product development, research, analytics, enforcing our [Terms of Service](#), and customer support purposes. For example, as part of our fraud prevention efforts, we scan and analyze messages to mask contact information and references to other sites, and subject to applicable law, we scan and analyze all images uploaded by users to the Airbnb platform in message threads, profiles, listings, and experiences for certain illegal or inappropriate activities (such as evidence of child exploitation) for the purpose of identifying and reporting content violations to appropriate authorities. In some cases, we may also scan, review, or analyze messages to debug, improve, and expand product offerings. We use automated methods where reasonably possible. Occasionally we may need to manually review communications, such as for fraud investigations and customer support, or to assess and improve the functionality of these automated tools. We will not review, scan, or analyze your messaging communications to send third-party marketing messages to you and we will not sell reviews or analyses of these communications. We may also share your communications as set out in the “Sharing & Disclosure” section.

3.5 Linking Third-Party Accounts.

You can link your Airbnb account with certain third-party services like social networks. Your contacts on these third-party services are referred to as “Friends.” When you direct the data sharing by creating this link:

- some of the information provided to us from linking accounts may be published on your public profile,
- your activities on the Airbnb Platform may be displayed to your Friends on the Airbnb Platform and/or that third-party service,
- a link to your public profile on that third-party service may be included in your Airbnb public profile,
- other Airbnb users may be able to see any Friends that you may have in common with them, or that you are a Friend of their Friend if applicable,

- other Airbnb users may be able to see any schools, hometowns, or other groups you have in common with them as listed on your linked social networking service,
- information you provide to us from the linking of your accounts may be stored, processed, and transmitted for fraud prevention, security investigations, and risk assessment purposes, and
- publication and display of information that you provide to the Airbnb Platform through this linkage is subject to your settings and authorizations on the Airbnb Platform and the third-party service.

3.6 Provide Payment Services. Personal information is used to enable, or authorize third parties to use, Payment Services, such as to:

- detect and prevent money laundering, fraud, abuse, and security incidents, as well as conduct risk assessments,
- comply with legal and compliance obligations (such as anti-money laundering regulations and sanctions enforcement),
- enforce the Payment Terms and other payment policies, and
- provide and improve Payment Services.

4. SHARING & DISCLOSURE



If you reside outside of the United States, learn about safeguards we rely on for transferring personal information to recipients outside of the EEA [here](#).

4.1 Sharing With Your Consent or at Your Direction.

Where you provide consent, we share your information as described at the time of consent, such as when authorizing a third-party application or website to access your Airbnb account or participating in promotional activities by Airbnb partners or third parties.

Where permissible under applicable law, we may use certain information about you, such as your email address, that we share with social media platforms after de-identifying it to generate leads, drive traffic to Airbnb, or otherwise promote our products and services.

4.2 Sharing Between Members.

To help facilitate bookings or other interactions between Members (who may be located in, or use service providers located in, jurisdictions with varying levels of data protection), we may share information in situations such as:

- Between Guest(s) and Host(s) when:
 - A booking request is made, when there is a co-host, or a dispute is submitted, such as profile, name, names of any additional Guests, cancellation history, review information, age of guest (unless prohibited by applicable law), dispute outcome (when applicable), and other information you choose to share and submit.
 - A booking is confirmed, additional information is shared to assist with coordinating the trip, such as profile photo and phone number.
 - You as a Host have a confirmed booking, certain information is shared with the Guest (and any additional Guests they invite, if applicable) to coordinate the booking, such as your profile, full name, phone number, and Listing address.
 - You communicate with a Member, such as your name, profile picture, and message content.
- Between Guests when:
 - You as a Guest invite additional Guests to a booking, certain information is shared with each additional Guest, such as your name, travel dates, Host name, Listing details, Accommodation address, and other related information.
- Between Hosts when:
 - You accept an invitation to host with another Member, you authorize those other Member(s), such as co-Hosts, to access and update your information and Member Content, such as certain information like your full name, phone number, Listing address, calendar, Listing information, Listing photos, and email address.

4.3 Information You Publish in Profiles, Listings, and Other Public Information.

You can make certain information publicly visible to others, such as:

- Your public profile page, which includes your profile photo, first name (or initials where applicable), description, and city.

- Listing pages that include information such as the Accommodation or Experience's approximate or precise location description, calendar availability, profile photo, aggregated demand information (like page views over a period of time), and additional information you choose to share.
- Reviews, ratings, and other public feedback.
- Content in a community or discussion forum, blog, or social media post.

We may display parts of your public profile and other Content you make available to the public like Listing details on third-party sites, platforms, and apps.

Information you share publicly on the Airbnb Platform may be indexed through third-party search engines. In some cases, you may opt-out of this feature in your account settings.

4.4 Host Service Providers.

Hosts may use third-party services to help manage or deliver their services, such as cleaning services or lock providers. Hosts may use features on the Airbnb Platform to share information about the Guest (like check-in and check-out information, Guest name, Guest phone number) with such third-party service providers.

4.5 Complying with Law, Responding to Legal Requests, Preventing Harm and Protecting Our Rights.

We may disclose your information to courts, law enforcement, governmental or public authorities, tax authorities, authorized third parties, or other Members, if and to the extent we are required or permitted to do so by law or where disclosure is reasonably necessary to: (i) comply with our legal obligations, (ii) comply with a valid legal request (such as a subpoena or court order) or to respond to claims asserted against Airbnb, (iii) respond to a valid legal request relating to a criminal investigation to address alleged or suspected illegal activity, or to respond to or address any other activity that may expose us, you, or any other of our users to legal or regulatory liability (more information on Airbnb's Law Enforcement Guidelines [here](#)), (iv) enforce and administer our agreements with Members, including our Terms, Additional Legal Terms, and Policies, or (v) protect the rights, property or personal safety of Airbnb, its employees, its Members, or members of the public.

Where appropriate, we may notify Members about legal requests unless: (i) providing notice is prohibited by the legal process itself, by court order we receive, or by applicable law, or (ii) we believe that providing notice would be futile, ineffective, create a risk of injury or bodily harm to an individual or group, or create or increase a risk of

fraud upon or harm to Airbnb, our Members, or expose Airbnb to a claim of obstruction of justice.

Where legally required or permissible according to applicable law, we may disclose Hosts' and/or Guests' information to tax authorities or other governmental agencies for the purpose of the tax authorities' determination of proper compliance with relevant tax obligations. Relevant tax obligations include Airbnb's tax obligations on its service fees, its facilitation of taxes on accommodations and withholding taxes, and Hosts' individual tax obligations. Information that may be disclosed includes, but is not limited to, Host and Guest names, listing addresses, Host addresses, tax/business identification number(s), date of birth, and/or contact information, property parcel identification numbers, payout information, transaction dates and amounts, number of nights and Guests booked, gross and net booking value and payout amounts, taxes collected by Airbnb on behalf of Guests and Hosts, to the extent any of this information is known by Airbnb.

In jurisdictions where Airbnb facilitates or requires a registration, notification, permit, or license application or number of a Host with a governmental authority, we may share information of participating Hosts with the relevant authority, both during the application process, when the Listing is published, and periodically thereafter, such as the Host's full name and contact details, Accommodation address, tax identification number, registration, permit, or license number, Listing details, reservation information, and number of nights booked subject to applicable laws.

4.6 Programs with Managers and Owners.

We may share personal information of Hosts and Guests with landlords, management companies, homeowners' associations, property owners, and/or property managers ("Building Management"), such as booking information and information related to compliance with applicable laws, in order to facilitate programs with Building Management. For example, guest booking and personal information, including guest contact information, may be shared with the Building Management of the building, complex, or community where a host lives and/or the listing is located to facilitate hosting services, compliance with applicable laws, security, billing, and other services.

4.7 Host Information Provided to Airbnb for Work Customers.

If a booking is designated as being for a business or work purpose and (1) is made by a Guest affiliated with an Enterprise and (2) the Enterprise is enrolled in Airbnb for Work, we may disclose information related to the booking to the Enterprise (e.g., name of the Host, Accommodation address, booking dates, Listing details, etc.) to the extent necessary for the adequate performance of Airbnb's contract with the Enterprise and

to provide the services. At the request of the Enterprise or the Guest, we may also share this information with third parties engaged by the Enterprise to provide support services.

4.8 Service Providers.

We share personal information with affiliated and unaffiliated service providers (including their service providers) to help us run our business and for their compliance purposes, including those that help us: (i) verify your identity or authenticate your identification documents, (ii) check information against public databases, (iii) conduct background checks, fraud prevention, security investigations, and risk assessments, (iv) perform product development, maintenance, and debugging, (v) allow the provision of the Airbnb Services through third-party platforms and software tools (e.g., through the integration with our APIs), (vi) provide customer service, advertising, or payments services, (vii) offer additional services you select, (viii) process, handle, or assess insurance claims or similar claims, or (ix) review, scan, and analyze communications on the Airbnb Platform for certain purposes (such as evidence of child exploitation). See the Analyzing and Sharing Your Communications section for additional information. These providers are contractually bound to protect your personal information and have access to your personal information to perform these tasks. Other Members can use services other than Airbnb to process your data. These can include email or reservation management software. Such services are outside of Airbnb's control and will be subject to applicable laws around the world with varying levels of data protection.

4.9 Business Transfers.

If Airbnb undertakes or is involved in any merger, acquisition, reorganization, sale of assets, bankruptcy, or insolvency event, then we may sell, transfer, or share some or all of our assets, including your information in connection with such transaction or in contemplation of such transaction (e.g., due diligence). In this event, we will notify you before your personal information is transferred and becomes subject to a different privacy policy.

4.10 Corporate Affiliates.

To support us in providing, integrating, promoting and improving the Airbnb Platform, Payment Services, and our affiliates' services, we may share personal information within our corporate family of companies that are related by common ownership or control. Some examples are:

- **Sharing with Airbnb, Inc.** Even if your country of residence is not the United States, your information will be shared with Airbnb, Inc., which provides the technical infrastructure for the Airbnb Platform.

- **Sharing with Airbnb Payments.** In order to facilitate payments on or through the Airbnb Platform, certain information as described in the “Outside of the United States” section will be shared with the relevant Airbnb Payments entity.
- **Sharing with Airbnb Ireland.** Even if your country of residence is outside EEA (e.g., United States, Japan, China) your information may be shared with Airbnb Ireland, which provides customer support and other business operation services to other Airbnb entities and may be disclosed in line with section 4.5 above.
- **Sharing with Airbnb GSL.** Even if your country of residence is not Japan, your information may be shared with Airbnb GSL, which provides customer support and other business operation services to other Airbnb entities.
- **Sharing with Airbnb China.** If you (i) created a Listing in China, (ii) inquired about or booked a Host Service located in China, or (iii) sent a message to a Host in relation to that Host’s listing in China, information you provided was shared with Airbnb China as described in the prior version of this Privacy Policy. Similar to other hospitality or short-term rental companies that do business in China, Airbnb China may disclose your information to Chinese government agencies without further notice to you. Your information may be further shared with service providers (including in China) to help run our business. Our service providers may also disclose your information where required by law.

5. OTHER IMPORTANT INFORMATION

5.1 Third-Party Partners & Integrations.

Parts of Airbnb may link to third-party services. Airbnb does not own or control these third parties. When you interact with these third parties and choose to use their service, you are providing your information to them. Your use of these services is subject to the privacy policies of those providers, including Google Maps/Earth Additional Terms of Use, Google Privacy Policy (see [here](#) for more information on how Google uses information), Paypal Privacy Statement, and Citi Privacy Policy.

6. YOUR RIGHTS

You can exercise any of the rights described in this section consistent with applicable law. See [here](#) for information on data subject rights requests and how to submit a request. We may ask you to verify your identity and request before taking further action on your request.

- 🌐 Learn more about rights under the General Data Protection Regulation (“GDPR”) and the Brazil General Data Protection Law (“LGPD”) [here](#).
If your country of residence is China, learn more about your rights [here](#).

6.1 Managing Your Information.

You can access and update some of your personal information through your Account settings. If you connected your Airbnb Account to a third-party service, like Facebook or Google, you can change your settings and unlink from that service in your Account settings. You are responsible for keeping your personal information up to date.

6.2 Data Access and Portability.

In some jurisdictions, applicable law may entitle you to request certain copies of your personal information or information about how we handle your personal information, request copies of personal information that you have provided to us in a structured, commonly used, and machine-readable format, and/or request that we transmit this information to another service provider (where technically feasible).

6.3 Data Erasure.

In some jurisdictions, you can request that your personal information be deleted. Please note that if you request deletion of your personal information, or if your account is suspended, terminated, or voluntarily closed:

- We may retain your personal information as necessary for our legitimate business interests, such as prevention of money laundering, fraud detection and prevention, and enhancing safety. For example, if we suspend an Airbnb Account for fraud or safety reasons, we may retain information from that Airbnb Account to prevent that Member from opening a new Airbnb Account in the future.
- We may retain and use your personal information to the extent necessary to comply with our legal obligations. For example, Airbnb and Airbnb Payments may keep information for tax, legal reporting, and auditing obligations.
- Information you have shared with others (e.g., Reviews, forum postings) may continue to be publicly visible on Airbnb, even after your Airbnb Account is canceled.
- Because we take measures to protect data from accidental or malicious loss and destruction, residual copies of your personal information may not be removed

from our backup systems for a limited period of time.

7. SECURITY

While no organization can guarantee perfect security, we are continuously implementing and updating administrative, technical, and physical security measures to help protect your information against unlawful or unauthorized access, loss, destruction, or alteration.

8. CHANGES TO THIS PRIVACY POLICY

We reserve the right to modify this Privacy Policy at any time in accordance with applicable law. If we do so, we will post the revised Privacy Policy and update the “Last Updated” date at the top. In case of material changes, we will also provide you with notice of the modification by email at least thirty (30) days before the effective date. If you disagree with the revised Privacy Policy, you can cancel your Account. If you do not cancel your Account before the date the revised Privacy Policy becomes effective, your continued access to or use of the Airbnb Platform will be subject to the revised Privacy Policy.

9. CONTACT INFORMATION AND RESPONSIBLE AIRBNB ENTITIES

For questions or complaints about this Privacy Policy or Airbnb’s handling of personal information (i) If you reside in the United States contact Airbnb, Inc., Legal Privacy, 888 Brannan Street, San Francisco, CA 94103 USA or by emailing us at dpo@airbnb.com or by calling us toll-free at (844) 234-2500; (ii) for payments related matter please use the contact information provided in the **Payments Terms of Service** page, and (iii) if you reside outside the United States, please use the contact information for your controller provided in the **Outside of the United States** page.

Review the [previous version of this page](#).

Related articles

Guest

[**Protecting your privacy**](#)

To create an environment that promotes not only physical safety, but also the safety and security of private information, certain behaviors ...

Guest

Airbnb and your personal info

Most data associated with your user account is deleted when you close your Airbnb account. However, some data is kept longer as required or ...

Privacy Policy for the United States

Please review our Privacy Policy.

Support

[Help Center](#)

[AirCover](#)

[Supporting people with disabilities](#)

[Cancellation options](#)

[Our COVID-19 Response](#)

[Report a neighborhood concern](#)

Community

[Airbnb.org: disaster relief housing](#)

[Combating discrimination](#)

Hosting

[Airbnb your home](#)

[AirCover for Hosts](#)

[Explore hosting resources](#)

[Visit our community forum](#)

[How to host responsibly](#)

[Airbnb-friendly apartments](#)

Airbnb

[Newsroom](#)

[Learn about new features](#)

[Letter from our founders](#)

[Careers](#)

[Investors](#)

[Gift cards](#)

 English (US) \$ USD

© 2023 Airbnb, Inc.

[Terms](#) · [Sitemap](#) · [Privacy](#) · [Your Privacy Choices](#) 



How TikTok is supporting our community through COVID-19

U.S.

Privacy Policy

Last updated: January 1, 2023

This Privacy Policy applies to TikTok services (the “Platform”), which include TikTok apps, websites, software and related services accessed via any platform or device that link to this Privacy Policy. The Platform is provided and controlled by TikTok Inc. (“TikTok”, “we” or “us”). We are committed to protecting and respecting your privacy. This Privacy Policy explains how we collect, use, share, and otherwise process the personal information of users and other individuals age 13 and over in connection with our Platform. For information about how we collect, use, share, and otherwise process the personal information of users under age 13 (“Children”), please refer to our [Children’s Privacy Policy](#).

Capitalized terms that are not defined in this Privacy Policy have the meaning given to them in the [Terms of Service](#).

- What Information We Collect
- How We Use Your Information
- How We Share Your Information
- Your Rights
- Your Choices
- Data Security and Retention
- Children and Teens
- Other Rights



What Information We Collect

What Information We Collect

We may collect information from and about you, including information that you provide, information from other sources, and automatically collected information.

Information You Provide

When you create an account, upload content, contact us directly, or otherwise use the Platform, you may provide some or all of the following information:

- Account and profile information, such as name, age, username, password, language, email, phone number, social media account information, and profile image.
- User-generated content, including comments, photographs, livestreams, audio recordings, videos, text, hashtags, and virtual item videos that you choose to create with or upload to the Platform (“User Content”) and the associated metadata, such as when, where, and by whom the content was created. Even if you are not a user, information about you may appear in User Content created or published by users on the Platform. When you create User Content, we may upload or import it to the Platform before you save or post the User Content (also known as pre-uploading), for example, in order to recommend audio options, generate captions, and provide other personalized recommendations. If you apply an effect to your User Content, we may collect a version of your User Content that does not include the effect.
- Messages, which include information you provide when you compose, send, or receive messages through the Platform’s messaging functionalities. They include messages you send through our chat functionality when communicating with merchants who sell goods to you, and your use of virtual assistants when purchasing items through the Platform. That information includes the content of the message and information about the message, such as when it was sent, received, or read, and message participants. Please be aware that messages you choose



What Information We Collect



or choose to paste content from the clipboard onto the Platform, we access this information stored in your clipboard in order to fulfill your request.

- Purchase information, including payment card numbers or other third-party payment information (such as PayPal) where required for the purpose of payment, and billing and shipping address. We also collect information that is required for extended warranty purposes and your transaction and purchase history on or through the Platform.
- Your phone and social network contacts, with your permission. If you choose to find other users through your phone contacts, we will access and collect information such as names, phone numbers, and email addresses, and match that information against existing users of the Platform. If you choose to find other users through your social network contacts, we will collect your public profile information as well as names and profiles of your social network contacts.
- Your choices and communication preferences.
- Information to verify an account such as proof of identity or age.
- Information in correspondence you send to us, including when you contact us for support.
- Information you share through surveys or your participation in challenges, research, promotions, marketing campaigns, events, or contests such as your gender, age, likeness, and preferences.

Information From Other Sources

We may receive the information described in this Privacy Policy from other sources, such as:

- If you choose to sign-up or log-in to the Platform using a third-party service such as Facebook, Twitter, Instagram, or Google, or link your TikTok account to a third-party service, we may collect information from the service—for example, your public profile information (such as nickname), email, and contact list.
- Advertisers, measurement and other partners share information with us about you and the actions you have taken outside of the Platform, such as your activities on other websites and apps or in stores, including the products or services you purchased, online or in person. These partners also share information with us, such as mobile identifiers for advertising, hashed email



What Information We Collect

- We may obtain information about you from certain affiliated entities within our corporate group, including about your activities on their platform.
- We may receive information about you from others, including where you are included or mentioned in User Content, direct messages, in a complaint, appeal, request or feedback submitted to us, or if your contact information is provided to us. We may collect information about you from other publicly available sources.

Automatically Collected Information

We automatically collect certain information from you when you use the Platform, including internet or other network activity information such as your IP address, geolocation-related data, unique device identifiers, browsing and search history (including content you have viewed in the Platform), and [Cookies](#).

- **Usage Information.** We collect information regarding your use of the Platform and any other User Content that you generate through or upload to our Platform.
- **Device Information.** We collect certain information about the device you use to access the Platform, such as your IP address, user agent, mobile carrier, time zone settings, identifiers for advertising purposes, model of your device, the device system, network type, device IDs, your screen resolution and operating system, app and file names and types, keystroke patterns or rhythms, battery state, audio settings and connected audio devices. We automatically assign you a device ID and user ID. Where you log-in from multiple devices, we will be able to use information such as your device ID and user ID to identify your activity across devices. We may also associate you with information collected from devices other than those you use to log-in to the Platform.
- **Location Data.** We collect information about your approximate location, including location information based on your SIM card and/or IP address. In addition, we collect location information (such as tourist attractions, shops, or other points of interest) if you choose to add the location information to your User Content. With your permission, we may also collect precise location data (such as GPS).
- **Image and Audio Information.** We may collect information about the videos, images and audio that are a part of your User Content, such as identifying the objects and scenery that



What Information We Collect



U.S. laws, such as faceprints and voiceprints, from your User Content. Where required by law, we will seek any required permissions from you prior to any such collection.

- **Metadata.** When you upload or create User Content, you automatically upload certain metadata that is connected to the User Content. Metadata describes other data and provides information about your User Content that will not always be evident to the viewer. For example, in connection with your User Content the metadata can describe how, when, where, and by whom the piece of User Content was created, collected, or modified and how that content is formatted. It also includes information, such as your account name, that enables other users to trace back the User Content to your user account. Additionally, metadata includes data that you choose to provide with your User Content, e.g., any hashtags used to mark keywords to the video and captions.
- **Cookies.** We and our service providers and business partners use cookies and other similar technologies (e.g., web beacons, flash cookies, etc.) (“Cookies”) to automatically collect information, measure and analyze how you use the Platform, including which pages you view most often and how you interact with content, enhance your experience using the Platform, improve the Platform, provide you with advertising, and measure the effectiveness of advertisements and other content. We and our partners also use Cookies to promote the Platform on other platforms and websites. Cookies enable the Platform to provide certain features and functionality. Web beacons are very small images or small pieces of data embedded in images, also known as “pixel tags” or “clear GIFs,” that can recognize Cookies, the time and date a page is viewed, a description of the page where the pixel tag is placed, and similar information from your computer or device. To learn how to disable certain Cookies, see the “[Your Choices](#)” section below.

We may link your contact or account information with your activity on and off our Platform across all your devices, using your email or other log-in or device information. We may use this information to display advertisements on our Platform tailored to your interests, preferences, and characteristics.

We are not responsible for the privacy practices of our service providers and business partners, and the information practices of these service providers and business partners are not covered by this Privacy Policy.

We may aggregate or de-identify the information described above. Aggregated or de-identified data is not subject to this Privacy Policy.



What Information We Collect

As explained below, we use your information to improve, support and administer the Platform, to allow you to use its functionalities, and to fulfill and enforce our Terms of Service. We may also use your information to, among other things, show you suggestions, promote the Platform, and customize your ad experience.

We generally use the [Information We Collect](#) :

- To fulfill requests for products, services, Platform functionality, support and information for internal operations, including troubleshooting, data analysis, testing, research, statistical, and survey purposes and to solicit your feedback.
- To customize the content you see when you use the Platform. For example, we may provide you with services based on the country settings you have chosen or show you content that is similar to content that you have liked or interacted with.
- To send promotional materials from us or on behalf of our affiliates and trusted third parties.
- To improve and develop our Platform and conduct product development.
- To measure and understand the effectiveness of the advertisements we serve to you and others and to deliver advertising, including targeted advertising, to you on the Platform.
- To make suggestions and provide a customized ad experience.
- To support the social functions of the Platform, including to permit you and others to connect with each other (for example, through our Find Friends function), to suggest accounts to you and others, and for you and others to share, download, and otherwise interact with User Content posted through the Platform.
- To use User Content as part of our advertising and marketing campaigns to promote the Platform.
- To understand how you use the Platform, including across your devices.
- To infer additional information about you, such as your age, gender, and interests.



What Information We Collect

- To verify your identity in order to use certain features, such as livestream or verified accounts, or when you apply for a Pro Account, to ensure that you are old enough to use the Platform (as required by law), or in other instances where verification may be required.
- To communicate with you, including to notify you about changes in our services.
- To announce you as a winner of our contests or promotions if permitted by the promotion rule, and to send you any applicable prizes.
- To enforce our Terms of Service, Community Guidelines, and other conditions and policies.
- Consistent with your permissions, to provide you with location-based services, such as advertising and other personalized content.
- To train and improve our technology, such as our machine learning models and algorithms.
- To combine all the [Information We Collect](#) we receive about you for any of the foregoing purposes.
- To facilitate sales, promotion, and purchases of goods and services and to provide user support.
- For any other purposes disclosed to you at the time we collect your information or pursuant to your consent.

How We Share Your Information

We are committed to maintaining your trust, and while TikTok does not sell your personal information or share your personal information with third parties for purposes of cross-context



What Information We Collect

We share the categories of personal information listed above with service providers and business partners to help us perform business operations and for business purposes, including research, payment processing and transaction fulfillment, database maintenance, administering contests and special offers, technology services, deliveries, sending communications, advertising and marketing services, analytics, measurement, data storage and hosting, disaster recovery, search engine optimization, and data processing. These service providers and business partners may include:

- Payment processors and transaction fulfillment providers, who may receive the [Information You Provide](#), [Information From Other Sources](#), and [Automatically Collected Information](#) but who do not receive your message data, including, in particular, the following third-party payment providers/processors: PayPal (<https://www.paypal.com/us/webapps/mpp/ua/privacy-full>) and Stripe (<https://stripe.com/en-ie/privacy>).
- Customer and technical support providers, who may receive the [Information You Provide](#), [Information From Other Sources](#), and [Automatically Collected Information](#).
- Researchers who may receive the [Information You Provide](#), [Information From Other Sources](#), and [Automatically Collected Information](#) but would not receive your payment information or message data.
- Advertising, marketing, and analytics vendors, who may receive the [Information You Provide](#), [Information From Other Sources](#), and [Automatically Collected Information](#) but would not receive your payment information or message data.

Within Our Corporate Group

We may share all of the [Information We Collect](#) with a parent, subsidiary, or other affiliate of our corporate group.

In Connection with a Sale, Merger, or Other Business Transfer



What Information We Collect

For Legal Reasons

We may disclose any of the [Information We Collect](#) to respond to subpoenas, court orders, legal process, law enforcement requests, legal claims, or government inquiries, and to protect and defend the rights, interests, safety, and security of the Platform, our affiliates, users, or the public. We may also share any of the [Information We Collect](#) to enforce any terms applicable to the Platform, to exercise or defend any legal claims, and comply with any applicable law.

With Your Consent

We may share your information for other purposes pursuant to your consent or at your direction.

We partner with third-party services (such as Facebook, Instagram, Twitter, and Google) to offer you a seamless sign-up, log-in, and content-sharing experience. We may share information about you with these third-party services if you choose to use these features. For example, the services may receive information about your activity on the Platform and may notify your connections on the third-party services about your use of the Platform, in accordance with their privacy policies. If you choose to allow a third-party service to access your account, we will share certain information about you with the third party. Depending on the permissions you grant, the third party may be able to obtain your account information and other information you choose to provide.

If you choose to engage in public activities on the Platform, you should be aware that any information you share may be read, collected, or used by other users. You should use caution in disclosing personal information while using the Platform. We are not responsible for the information you choose to submit.

When you make a purchase from a third party on the Platform, including from a merchant selling products through our shopping features, we share the information related to the transaction with that third party and their service providers and transaction fulfillment providers. By making the purchase, you are directing us to share your information in this way. These entities may use the information shared in accordance with their privacy policies.



What Information We Collect

You may submit a request to know, access, correct or delete the information we have collected about you at <https://www.tiktok.com/legal/report/privacy>. You may appeal any decision we have made about your request by following the instructions in the communication you receive from us notifying you of our decision. You may also exercise your rights to know, access, correct, delete, or appeal by sending your request to the physical address provided in the “[Contact Us](#)” section below. You can also update your account information directly through your in-app settings, as well as request a copy of your TikTok data or request to deactivate or delete your account. Your right to know includes what personal information we have collected about you, including the categories of sources from which the personal information is collected, the business or commercial purpose for collecting or sharing personal information, the categories of third parties to whom we share the personal information, and the specific pieces of personal information we have collected about you. We do not discriminate based on the exercise of any privacy rights that you might have.

You may be entitled, in accordance with applicable law, to submit a request through an authorized agent. To designate an authorized agent to exercise choices on your behalf, please provide evidence that you have given such agent power of attorney or that the agent otherwise has valid written authority to submit requests to exercise rights on your behalf. We will respond to your request consistent with applicable law and subject to proper verification. We will verify your request by asking you to send it from the email address associated with your account or to provide information necessary to verify your account.

The metrics for requests to access, correct, and delete received by TikTok during the previous calendar year can be found [here](#).

While some of the information that we collect and use may constitute sensitive personal information, we only process such information in order to provide the Platform and within other exemptions under applicable law. For example, we may process your financial information in order to provide you the goods or services you request from us or your driver's license number in order to verify your identity.



What Information We Collect

- You may be able to control some of the **Information We Collect** through your device browser settings to refuse or disable **Cookies**. Because each browser is different, please consult the instructions provided by your browser. Please note that you may need to take additional steps to refuse or disable certain types of Cookies. In addition, your choice to disable Cookies is specific to the particular browser or device that you are using when you disable Cookies, so you may need to separately disable Cookies for each type of browser or device. If you choose to refuse, disable, or delete Cookies, some of the functionality of the Platform may no longer be available to you. Without this information, we are not able to provide you with all of the requested services.
- You can navigate to "Ads" in your in-app settings to opt-out of targeted advertising based on personal information about your activity on nonaffiliated apps and websites.
- You may be able to manage third-party advertising preferences for some of the third parties we work with to serve advertising across the Internet by using the choices available at https://www.networkadvertising.org/managing/opt_out.asp and <https://www.aboutads.info/choices>.
- Your device may have controls that determine what **Information We Collect**. For example, you can control whether we can collect your mobile advertising identifier for advertising through settings on your Apple and Android devices.
- You can opt out of marketing or advertising emails by using the “unsubscribe” link or mechanism noted in marketing or advertising emails.
- If you previously chose to share precise location information, you can prevent your device from sharing precise location information (e.g., GPS location information) with the Platform at any time through your device’s operating system settings.
- If you have registered for an account, you may access, review, and update certain personal information that you have provided to us by logging into your account and using available features and functionalities.
- Some browsers transmit “do-not-track” signals to websites. Because of differences in how browsers incorporate and activate this feature, we currently do not take action in response to



What Information We Collect



Data Security and Retention

We use reasonable measures to help protect information from loss, theft, misuse, unauthorized access, disclosure, alteration, or destruction. You should understand that no data storage system or transmission of data over the Internet or any other public network can be guaranteed to be 100 percent secure. Please note that information collected by third parties may not have the same security protections as information you submit to us, and we are not responsible for protecting the security of such information.

We retain information for as long as necessary to provide the Platform and for the other purposes set out in this Privacy Policy. We also retain information when necessary to comply with contractual and legal obligations, when we have a legitimate business interest to do so (such as improving and developing the Platform, and enhancing its safety, security and stability), and for the exercise or defense of legal claims.

The retention periods are different depending on different criteria, such as the type of information and the purposes for which we use the information. For example, when we process your information such as your profile information to provide you with the Platform, we keep this information for as long as you have an account. If you violate our Terms of Service, Community Guidelines, or other conditions or policies, we may remove your profile immediately, but may keep other information about you to process the violation.

TikTok may transmit your data to its servers or data centers outside of the United States for storage and/or processing. Other entities with whom TikTok may share your data as described herein may be located outside of the United States.



What Information We Collect

The privacy of Children is important to us. We provide a separate experience for Children in the United States, in which we collect and process only limited information. For information about how we collect, use, share, and otherwise process the personal information of Children, please refer to our [Children's Privacy Policy](#).

The Platform otherwise is not directed at Children. If we become aware that personal information has been collected on the Platform from a Child, we will delete this information and terminate the Child's account. If you believe there is a user who is below the age of 13, please contact us at: <https://tiktok.com/legal/report/privacy>.

If you are a parent or guardian, our [Guardian's Guide](#) contains information and resources to help you understand the Platform and the tools and controls you can use.

Other Rights

Sharing for Direct Marketing Purposes (Shine the Light)

If you are a California resident, once a calendar year, you may be entitled to obtain information about personal information that we shared, if any, with other businesses for their own direct marketing uses. To submit a request, contact us at: <https://www.tiktok.com/legal/report/privacy>.

Content Removal for Users Under 18



What Information We Collect



We may not be able to respond if you do not provide adequate information. Please note that your request does not ensure complete or comprehensive removal of the material. For example, User Content that you have posted may be republished or reposted by another user.

Privacy Policy Updates

We may update this Privacy Policy from time to time. When we update the Privacy Policy, we will notify you by updating the “Last Updated” date at the top of the new Privacy Policy, posting the new Privacy Policy, or providing any other notice required by applicable law. We recommend that you review the Privacy Policy each time you visit the Platform to stay informed of our privacy practices.

Contact Us

Questions, comments and requests regarding this Privacy Policy should be addressed to:

- Contact us: <https://www.tiktok.com/legal/report/privacy>
- Mailing Address: TikTok Inc., Attn: Privacy Policy Inquiry, 5800 Bristol Parkway, Suite 100, Culver City, CA 90230



What Information We Collect



Company

[About TikTok](#)

[Newsroom](#)

[Contact](#)

[Careers](#)

[ByteDance](#)

Programs

[TikTok for Good](#)

[TikTok for Developers](#)

[Effect House](#)

[Advertise on TikTok](#)

[TikTok Browse](#)

[TikTok Embeds](#)

[TikTok Rewards](#)

Resources

[Help Center](#)

[Safety Center](#)

[Creator Portal](#)

[Community Guidelines](#)

[Transparency](#)

[Accessibility](#)

Legal

[Terms of Service](#)



[TIKTOK PLATFORM COOKIES POLICY](#)

What Information We Collect



© 2023 TikTok

Three Milestones in the History of Privacy in the United States

Vernon Valentine Palmer*

I.	INTRODUCTION	67
II.	A FIRST MILESTONE: WARREN AND BRANDEIS'S INVENTION OF PRIVACY	70
	<i>A. Intervening Years 1890-1970</i>	79
III.	A SECOND MILESTONE: PROSSER'S REFORMULATION OF PRIVACY	82
	<i>A. Prosser's Methodology Revisited</i>	85
	<i>B. Finding Order, Losing Sight of Privacy</i>	89
	<i>C. The Four Privacies Enter American Common Law</i>	91
IV.	THE THIRD MILESTONE: THE CONSTITUTIONAL TRANSFORMATION OF LIBERTY INTO PRIVACY	93
V.	CONCLUSION	97

I. INTRODUCTION

The subject of privacy rights fits somewhere within the far broader subject of personality rights. Personality rights of course are numerous and diffuse. As Jean Dabin defined them, they are “rights whose subject is the component elements of the personality considered in its manifold aspects, physical and moral, individual and social.”¹ They may be classified by general headings under which related interests are grouped together. On the Continent and in countries where a general theory of personality rights has developed, privacy will be regarded as one of the individual’s social personality rights. It is only one of many personality interests that the law should protect. The rights relating to the physical and affective personality receive separate consideration.²

* Thomas Pickles Professor of Law and Co-Director of the Eason Weinmann Center for Comparative Law. This Article was first presented in draft to the Conference on Tort Law held in Shanghai on October 14-15, 2010.

1. Quoted (as translated) in Gert Bruggemeier, *Protection of Personality Interests in Continental Europe: The Examples of France, Germany and Italy, and a European Perspective*, in Niall Whitty & Reinhard Zimmermann (eds.), *RIGHTS OF PERSONALITY IN SCOTS LAW—A COMPARATIVE PERSPECTIVE* (Dundee U.P. 2009) [hereinafter WHITTY & ZIMMERMANN].

2. Swiss law, for example, presents the following tableau:

In the United States, however, where the phrase “personality rights” suffers from unfamiliar resonance and disconcerting generality, the law of privacy has developed fitfully, without the benefit of general theory and with little attention to taxonomy.³ In the unstructured environment of case-by-case development, understandably the concept has taken on unusual meanings. Certainly today it means more than *la vie privée* or privacy in a narrow sense.⁴ During the course of more than a 120 year development it somehow acquired, absorbed and incorporated various tangential interests such as the right to control use of one’s name, one’s image, one’s writings, one’s life story, and even the right to exploit one’s own publicity value. Obviously those who seek to capitalize upon the publicity value of their name or talent are not in fact seeking privacy in the usual sense of the word, and yet American tort law protects the publicity right either in the name of privacy or describes it as a related offshoot. Somewhat more remarkable is that our Supreme Court, in the name of protecting “privacy,” has swept together various liberties not expressly stated in the Constitution, like the decision freely to marry, the

-
- I. Rights of the physical personality
 - Right to life
 - Right of corporeal integrity
 - Liberty of movement
 - Sexual Liberty
 - Protection of the body after death
 - II. Rights of the affective personality
 - Right to relations with loved ones
 - Right to respect for loved ones
 - Right to conjugal sentiments
 - Right to family heirlooms
 - III. Rights of the social personality
 - Right to name and other identifying signs
 - Right to one’s image and voice
 - Right to private life

See PIERRE TERCIER, LE NOUVEAU DROIT DE LA PERSONNALITÉ (Schulthess 1984) (my translation). On French law, see E.H. Perreau, *Des droits de la personnalité*, 8 RTDC 501 (1909); RAYMOND LINDON, LES DROITS DE LA PERSONNALITÉ (Dalloz 1974); PIERRE KAYSER, LA PROTECTION DE LA VIE PRIVÉE (3ed Economica 1995); JEAN CARBONNIER, DROIT CIVIL 1/LES PERSONNES (Thémis 2000).

3. There has been limited discussion. See Roscoe Pound, *Interests of Personality*, 28 HARV. L. REV. 343 (1915); Leon Green, *The Right of Privacy*, 27 ILL. L. REV. 237 (1932). Green’s scheme of personality interests recognized seven categories: physical integrity, feelings or emotions, capacity for activity or service, name, likeness, history and privacy.

4. Compare the more limited meaning and scope of privacy under the European Human Rights Convention: “Art. 8 Right to respect for private and family life. 1. Everyone has the right to respect for his private and family life, his home and his correspondence.”

right to procreate, the freedom to have an abortion or not, to educate one's children in a foreign language and so forth. These rights, important as they are, are not exercised in private but in public settings, as in public schools, public hospitals, and churches. Such rights and liberties do fall somewhere on an inclusive tableau of personality rights,⁵ but the question remains: are they aspects of privacy? Why should they be called "privacy"? If privacy is supposed to mean all these things, in tort law and constitutional law, how can it be defined? My paper does not dwell upon the definitional question. It merely assumes that privacy cannot be defined coherently to mean so many things. It simply asserts that privacy in the United States is now an umbrella concept under which diffuse personality interests are brought together. I believe that how this came about is interesting and to understand the development we must follow the course of the development of this intriguing concept back to its beginnings in American law.

This paper can only retell a few chapters of the story of privacy in the United States.⁶ I think you will find it is not like the story in France, where the judges built an impressive jurisprudence upon a Roman foundation in the 19th century,⁷ nor is it anything like the story in Germany where the fathers of the BGB turned their backs upon the Roman heritage and banished personality rights from the civil law, only to see them later return under the Bonn Constitution.⁸ Nor is it even similar to the English story where personality rights and privacy itself remain somewhat unfamiliar and unrecognized concepts.⁹ Compared to the paths of European privacy, the United States has followed a unique trajectory, and compared to the concept of privacy on the Continent, it is a *sui generis* creation.

I will discuss three milestones in this 120 year journey. The first was the original treatment of the subject by Samuel Warren and Louis

5. In the Swiss tableau in note 3 above, these diverse liberties come under headings I and II.

6. No attempt has been made to cover the myriad federal and state statutes in the United States dealing with protection of privacy. For an overview, see JOHN SOMA & STEPHEN RYNERSON, *PRIVACY LAW IN A NUTSHELL* 74-185 (2008), and DANIEL J. SOLOVE, *UNDERSTANDING PRIVACY* (Harv. 2008).

7. See French authorities in Bruggemeier, *supra* note 1.

8. See Florian Wagner-von Papp & Jorg Fedtke, *Germany*, in Koziol & Steininger (eds.), *EUROPEAN TORT LAW 2008* (Springer 2008); HANS-JOACHIM CREMER, *HUMAN RIGHTS AND THE PROTECTION OF PRIVACY IN TORT LAW: A COMPARISON BETWEEN ENGLISH AND GERMAN LAW* (Cavendish 2011); Bruggemeier, *supra* note 1.

9. To this day invasion of privacy is not a recognized tort as such under English Common Law. See *Wainwright v. United Kingdom* [2007] 44 EHRR 40. The closest analogue would be the action for breach of confidence which appears to have recently undergone a name change. It is now called misuse of private information. *Campbell v. MGN* [2004] UKHL 22.

Brandeis in their famous article “The Right of Privacy,”¹⁰ in which the authors conceived of the need for such a right and through some combination of prestige and persuasion they set the American common law on an historical trajectory which turned out to be more far-reaching than in other common law jurisdictions. Following a seventy-year period of incubation and growth in which privacy rights received broad recognition, a second milestone was reached with the reformulation of the privacy right by William Prosser.¹¹ Prosser restructured all invasions of privacy into four separate torts and successfully implanted his own taxonomy directly into the Restatement 2nd of Torts. He effectively reshaped the landscape of American tort law until this day. The third milestone, which began in the 1960s and has by no means run its course, saw not only the application of constitutional limits on the common law torts, but the recognition of new constitutionally based privacy rights with origins independent of the common law. In the latter development, however, privacy encompasses a set of fundamental rights with little or nothing in common with the privacy protected by tort law. It concerns personality rights arising from the constitution, not a series of torts limited by the constitution. These rights protect against governmental rather than private invasion and require balancing of one constitutional right against another.

These milestones will provide a loose framework for an overview of this subject in which I hope to trace the progress and problems that privacy rights have encountered over the past century.

II. A FIRST MILESTONE: WARREN AND BRANDEIS’S INVENTION OF PRIVACY

Curiously the right of privacy in American law had its inception not in a case or a statute, but in a law review article. That is usually considered an inauspicious beginning for common law development, yet no one seems to doubt that privacy rights achieved “takeoff” in the United States because of the special attributes of this famous article.

Samuel Warren and Louis Brandeis were classmates at the Harvard Law School and had been law partners in Boston up until 1889, one year before the article’s publication. The immediate reason for their concern about privacy rights was probably heavy media coverage of the private affairs of Warren, a socially prominent Bostonian who had married into an important political family. According to William Prosser, they sought

10. Samuel Warren & Louis Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193 (1890).

11. William Prosser, *Privacy*, 48 CAL. L. REV. 383, 423 (1960).

to curb the prying eyes of the press, which had covered in great detail the comings and goings of Warren's family.¹² The article itself does not disclose or discuss in so many words the personal motives of the authors yet one widely quoted passage pointed to the excessive curiosity of the tabloid press:

The press is overstepping in every direction the obvious bounds of propriety and decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle. . . .¹³

In the context of the late nineteenth century these complaints about the press's disregard for privacy can be paired with similar complaints in other countries. Privacy had not found its way into the leading documents of the 18th century Enlightenment. Neither the American Constitution nor France's Declaration of the Rights of Man made any reference to it, apparently because there was as yet no formulated political or legal demand.¹⁴ Nor had it received any attention in the French Civil Code of 1804, or the BGB of 1900.¹⁵ Further, our more remote ancestors apparently had little interest or need for privacy, for as

12. Recent research has uncovered as many as 60 articles in New York, Washington and Boston newspapers which give details about Mrs. Warren's various parties, luncheons, and social affairs, including accounts of the funeral of Mrs. Warren's sister and her mother, and of her own marriage to Mr. Warren. See Amy Gajda, *What If Samuel D. Warren Hadn't Married A Senator's Daughter?: Uncovering the Press Coverage That Led to "The Right of Privacy,"* 2008 MICH. ST. L. REV. 35.

13. Warren & Brandeis, *supra* note 10. Prosser would lead us to believe that the motives for the piece may be traced to Warren and the intellectual contribution to Brandeis, but it is difficult to assess such assertions.

14. Of course the 3rd and 4th Amendments to the U.S. Constitution may be read as protecting privacy interests, but the protections were narrow and the word was not used.

15. Elspeth Reid notes, "Few of the issues of privacy and confidentiality which so concern us today troubled Portalis, or the fathers of the German Civil Code." Elspeth Reid, *Protection of Personality Rights in the Modern Scots Law of Delict*, in WHITTY & ZIMMERMANN, *supra* note 1, at 310. The clear trend of the 20th and 21st centuries, however, is to emphasize and enumerate personality rights in the Civil Codes. The Swiss Civil Code (1907)(its Book I contained the "Law of Personality") was of course first in line and was inspired by French court practice. For the more modern trend see the Civil Code of Quebec (1991), art. 3 ("Every person is the holder of personality rights, such as the right to life, the right to the inviolability and integrity of his person, and the right to the respect of his name, reputation and privacy.") and thereafter arts. 10-11, 35-37, 42, 55; the Civil Code of Czechoslovakia (1964) art. 11 ("A citizen is entitled to protection of his personality, in particular his life and health, civil honor, as well as his name and expressions of a personal nature."), and thereafter arts. 12-17. To my knowledge the most extensive treatment is to be found in the new Chinese Civil Code (2009) where an entire title consisting of seven chapters (Title IV Personality Right Law) is devoted to the subject.

E.L. Godkin asserted, “Privacy . . . is one of the luxuries of civilization, which is not only unsought for but unknown in primitive or barbarous societies. The savage cannot have privacy, and does not desire or dream of it.”¹⁶ Robinson Crusoe, it appears, had perfect privacy but neither he nor his contemporaries were actually seeking it. Society began to evidence prepolitical interest in privacy in the 18th century, as new architectural forms, home furnishings, diaries, letters and novels began to reflect a desire for intimacy.¹⁷ Arguably in 19th century America the right may have already existed for many well before Warren and Brandeis highlighted the issue. A physical intrusion on privacy, for example, was already considered a tort, and there were a variety of protections—e.g., criminal laws against peeping Toms, prohibitions against opening private letters in the mails and telegraph messages, protections for confidential disclosures to confessors, doctors and spouses, not to mention the Fourth Amendment guarantee against unreasonable search and seizure—all of which addressed the issue in piecemeal fashion.¹⁸

In the latter half of the century the demand for privacy may have quickened with the rise of the mass-circulation daily newspapers and the invention of “instantaneous photography.” Facilitated by the availability of hand-held cameras¹⁹ and other technological breakthroughs, photojournalism now became the standard accessory of the news reporter.²⁰ Photographs of those in the news were taken not only with greater ease, but often for illustrative purposes and without permission. The intrusive effect was apparently first felt by those who excited public curiosity the most, namely the noble families, political leaders and famous celebrities. Indeed the first cases we have were brought on behalf of towering figures like Chancellor Bismarck of Germany, Queen Victoria of England and the famous French actress Rachel.²¹ Of course

16. *The Rights of the Citizen: To His Reputation*, 8 SCRIBNER'S MAG. 58, 65 (1890)

17. See PATRICIA MEYER SPACKS, PRIVACY: CONCEALING THE EIGHTEENTH-CENTURY SELF (Chicago Press 2003); A. PARDAILHÉ, LA NAISSANCE DE L'INTIME (1988).

18. See Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892, 1895 (1981) (sacred “right of privacy” violated when doctor brought an unqualified assistant into the bedchamber of a woman in childbirth).

19. See Robert E. Mensel, “Kodakers Lying in Wait”: Amateur Photography and the Right of Privacy in New York, 1885-1915, 43 AM. Q. 24 (Mar. 1991).

20. The practice of illustrating news stories with photographs was made possible by printing and photography innovations between 1880 and 1897. While newsworthy events were photographed as early as the 1850s, presses could only publish from engravings until the 1880s. Early news photographs required that photos be reinterpreted by an engraver before they could be published.

21. Bismarck's case involved what we would now call in the United States the “intrusion” tort. On the evening of Bismarck's death (July 30, 1898), two photographers stole into his bedroom at 4 a.m. and took flash pictures of the prince in his deathbed, then offered to sell these

in one sense this dynamic has not fundamentally changed even if it is more democratized. The modern law of privacy continues to be driven by privacy-seeking, curiosity-inspiring celebrities. It seems fair to say that Warren and Brandeis's complaint fits the pattern of a watershed period when the privacy of the prominent was initially disturbed.

Given the relatively recent origins of the demand, the authors wisely made no attempt to claim that privacy was an ancient "natural right" or a liberty interest protected under the constitution. Nor did they boldly seek to be the first to delimit the meaning of privacy. As we know, they only borrowed the memorable phrase of Judge Cooley that it was the right "to be let alone".²² This left its meaning open to anyone's interpretation of what being left alone meant. Of course if we look closely at the authors' descriptions of privacy violations, their various arguments and hypotheticals, and the case authorities they considered relevant, it is possible to trace a more helpful outline of their thought. An inductive search through the article reveals they had several kinds of privacies in mind. The invasions apparently included the unauthorized "circulation of portraits" in the press and elsewhere;²³ the publication of "gossip" about domestic events; the unauthorized publication or display of private letters, works, creations,²⁴ and even lectures at the university;²⁵ the publishing of catalogues and lists of one's creations or possessions; intrusions into the domestic foyer to obtain private information,²⁶ including access by trespass or eavesdropping;²⁷ and finally the

to the press. At the family's request, the police confiscated the plates and the photographers received prison sentences. The photo was suppressed until 1952. See *Bismarck on His Deathbed*, iconicphotos.wordpress.com. A somewhat similar situation occurred after the death of Elisabeth "Rachel" Félix. The actress was photographed on her death bed with the permission of her sister, but on the express understanding that no copy was to be given to anyone else. Pencil drawings based on the photograph, however, were made and put up for sale. The family obtained a court order to have the drawings seized and destroyed. Félix v. O'Connell, 16 juin 1858, Trib. Civ de la Seine, 1ere Ch., D. 1858, 3.62. Prince Albert's and Queen Victoria's effort to prevent a gallery from displaying their amateur etchings is detailed in the case of *Prince Albert v. Strange 2 De Gex & Sm.* 652 (1849).

22. Warren & Brandeis, *supra* note 10, at 194.

23. "For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons. . ." *Id.* at 195.

24. Prince Albert v. Strange, *infra* note 8. (etchings by Queen Victoria for her private amusement).

25. Abernethy v. Hutchinson, 3 L.J. Ch. 209 (1825) (unpublished medical lectures).

26. "... idle gossip which can only be procured by intrusion upon the domestic circle." Warren & Brandeis, *supra* note 10, at 196.

27.

But can it be supposed that the court would hesitate to grant relief against one who had obtained his knowledge by an ordinary trespass—for instance, by wrongfully looking into a book in which the secret was recorded, or by eavesdropping? Indeed, in Yovatt v.

publication of secret and intimate knowledge in breach of confidence.²⁸ From these indicia, it seems they sought protection for at least three phases of the personality: (1) control over the use of one's name, likeness or photograph, (2) a reserved sphere of personal and family life, and (3) control over one's creations, writings and thoughts. In some respects their concept was spatial, as in emphasizing that the domestic circle and the sanctuary of the home were off-limits to information gathering. In other respects, however, it was non-spatial, as when the individual sought to prevent the circulation of her photograph or writings in the press. One side of the coin implied a limit on society's access to the individual²⁹ but the other called for the individual's right to control information or creations that were already in other people's hands.

Warren and Brandeis's article distinguishes itself, methodologically, by the boldness of its approach. They critiqued the existing common law (equity here included) by close attention to the underlying social interests protected by individual actions. The orthodox method of the common lawyer attempting to prove the existence of a right such as privacy would normally lead to analogizing judicial precedents and bending the forms of action. Warren and Brandeis, I submit, argued the matter the other way round. They treated the right to privacy as if it already existed. They spent no time debating this point.³⁰ It may be significant that their title was "The Right of Privacy" as opposed to "Is There a Right of Privacy?" The right stemmed from the underlying interests and needs of contemporary society,³¹ it was not sought in the marrow of the common law remedial system.³² They assumed the right's existence would precede

Winyard, 1 J. & W. 394 (1820), where an injunction was granted against making any use of or communicating certain recipes for veterinary medicine, it appeared that the defendant, who had been in plaintiff's employ, had surreptitiously gotten access to his book of recipes, and copied them. Lord Eldon "granted the injunction upon the ground of there having been a breach of trust and confidence;" but it would seem to be difficult to draw any sound legal distinction between such a case and one where a mere stranger wrongfully obtained access to the book.

Id. at 212.

28. Warren & Brandeis, *supra* note 10, at 211.

29. ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 10 (1988); E.L. Godkin, *Libel and Its Legal Remedy*, 12 J. SOC. SCI. 69, 80 (1880).

30. They essentially disregarded the mine of legal authorities collected in the Note, *supra* note 18.

31. The term "interest" is being used in the sense the Restatement of Torts Second uses the term, i.e., to denote an object of human desire (ALI 1977, § 1).

32. James Gordley observes as an historical matter that the later common law tort writers began a process of rationalizing and classifying the forms of action in terms of the interests each protected. In doing so, they made it sound as if someone in authority had actually decided what interests should be protected, when nothing of the kind had ever actually been decided. Arguing in a circle, the writers measured the scope of an interest by the scope of the individual action.

the common law's recognition of it. The common law might recognize the right but it did not create it.³³ Theirs therefore was a method of arguing from right to remedy rather than from remedy back to right. This argument (uncharacteristic of common lawyers) enabled them to concentrate upon showing how imperfectly the common law protected the privacy interest.

Their critique showed that privacy interests were not protected except as the indirect effect of protecting something else, for example in the course of protecting reputation or property rights. What protection there was for the privacy interest was always the oblique result of shoehorning plaintiff's facts into one of the older, recognized torts. For example an author's control over his literary and artistic compositions was already a recognized property right, but this had forced courts to distort the usual meaning of property. It was conceded that an artist's compositions certainly possess "many of the attributes" of ordinary property, but when the issue was not who should profit from works of this kind, but rather who has the right to control or prevent dissemination of private information with no intellectual or literary significance, the property theory hardly covered the real interest at stake. To use one of their examples, if a man's diary merely stated that he dined at home with his wife, it was difficult to regard this information as a form of property, at least not "in the common acceptation of that term." In such a case the real thing to be protected was simply a kind of private information. What judges had been calling the author's "property" would be more logically explained in terms of the right to privacy. Of course if one cared to stretch language as far as possible, it would indeed be possible to restate all interests (even that of bodily integrity or reputation) in terms of

FOUNDATIONS OF PRIVATE LAW: PROPERTY, TORT, CONTRACT, UNJUST ENRICHMENT 169 (OUP 2006). The tort writers never grounded those interests in social conditions, as Warren and Brandeis did. They instead assumed the common law was the source and that it supplied the scope of the protected interest. They rationalized these interests in an after-the-fact, circular, fashion. Warren and Brandeis posited a privacy interest before there were actions in privacy to rationalize.

33. Their approach resembles Pound's interest-oriented approach in *Interests of Personality*, where he states:

A legal system attains its end by recognizing certain interests,—individual, public, and social,—by defining the limits within which these interests shall be recognized legally and given effect through the force of the state. . . . It does not create these interests. . . . [T]hey arise, apart from the law, through the competition of individuals with each other, the competition of groups or societies with each other, and the competition of individuals with such groups or societies. The law does not create them, it only recognizes them.

Pound, *supra* note 3, at 343-44.

property, but surely this would denature the word and rob classification of all value.³⁴

They likewise showed that the actions for breach of contract, trust or confidence were equally limited in protecting private information. Actions of that kind presupposed the betrayal of some antecedent relationship of trust or perhaps the breach of a promise not to disclose private information about plaintiff. The action could not lie if the disclosure came from someone with whom plaintiff had no prior relationship, for example if disclosure was made by the press or some stranger from whom plaintiff had received no undertaking of confidentiality.³⁵ What was missing was protection *erga omnes* as opposed to an action which presupposed relational privity.³⁶ The law of libel and slander also offered inadequate piecemeal protection. Those actions dealt with reputational interests, the lowering of a person's estimation in the community, and thus affected the individual's external relations to the community. They had no reference to the humiliation or embarrassment or indignity caused by an invasion of privacy. The common law had no action equivalent to the Roman action for *injuria* which took feelings and man's spiritual side into account.³⁷ Indeed, so long as defendant published only true and accurate facts, or published private facts that would not necessarily lower plaintiff's reputation,

34. Leon Green once noted that if language is distorted sufficiently all legal interests (whether personality interests or interests in relations with others) could be restated as property interests. *See The Right of Privacy*, 27 ILL. L. REV. 237 (1932). He cited the statement of Vice Chancellor Malins in *Dixon v. Holden* (1869) L.R. 7 Eq. Cas. 488, as an example of this logic: "What is property? One man has property in lands, another in goods, another in business, another in skill, another in reputation; and whatever may have the effect of destroying property in any one of these (even in a man's good name) is in my opinion destroying property of a most valuable description." Green thought it would also be possible, though equally distortive, to try to protect property interests by stretching the language of personality interests or to protect both property and personality interests by classifying them as interests in relations with other persons.

35. These two criticisms were broadly applicable to, and were no doubt inspired by, the reasoning in the leading case of *Prince Albert v. Strange*, [1849] EWHC Ch J20, which Warren and Brandeis cited extensively. In that case drawings and etchings which Queen Victoria and Prince Albert had made for their own amusement were surreptitiously taken and ended up in the hands of defendant Strange who planned to exhibit them at his gallery. An injunction was issued to prevent the exhibition as well as to prohibit publication and sale of an exhibition catalogue describing the works. The plaintiffs' argument was wholly based upon protecting the Queen's and Prince's property in these unpublished works. The Lord Chancellor upheld the injunction on the ground of property and/or breach of trust. "Both appear to me to exist in this case."

36. The privity limitation on this action still applies in some American jurisdictions, *see, e.g.*, *Doe v. Portland Health Ctrs.*, 99 Or. App. 423, 782 P.2d 446 (1989), but has been removed at English common law. *See infra* note 45.

37. Warren & Brandeis, *supra* note 10, at 197 ("[O]ur law recognizes no principle upon which compensation can be granted for mere injury to the feelings.").

regardless how that might make plaintiff feel, an action for defamation would not lie. It could not vindicate the interest in privacy.

One further methodological point of interest is Warren and Brandeis's use of comparative law, in particular their reference to French legislation. France had arguably the most developed protection of privacy in late 19th century Europe. It impressed Godkin who wrote an influential social essay in 1880 that the authors had evidently absorbed.³⁸ Warren and Brandeis introduced the French experience quite laconically: "The right to privacy, limited as such right must necessarily be, has already found expression in the law of France." That assertion was true enough in 1890 and yet it was not based upon the rights which the courts of France had progressively recognized in the 19th century under the general clause of the Code Civil (art. 1382 CC). The authors made no allusion to the line of cases such as "l'affaire Rachel" (1858)³⁹ or "l'affaire Dumas" (1867)⁴⁰ in which the publication of private photographs was enjoined or caused liability.⁴¹ Surprisingly their assertion was based upon the "ephemeral" 1868 Press Act⁴² which imposed minor criminal sanctions for publishing "any fact of private life" in the newspaper. The curiosity is that this Act, which apparently had not been enforced by the government and indeed was repealed nine years before the Harvard article appeared, should be authority for France's recognition of the right of privacy. The explanation seems to be that the authors were less interested in the Act itself than the valuable ideas and instructions found in the Minister of Justice's Circular accompanying the Act. The Circular, from which they quoted several sections, advanced valuable ideas concerning how to balance and reconcile rights to the *vie privée* with freedom of the press. It offered concise guidelines how this right might operate consistent with the press's privileges and the defense of truth under actions for defamation. Brandeis and Warren leaned

38. E.L. Godkin, *Libel and Its Legal Remedy*, XLVI ATL. MONTHLY 729-38 (Dec. 1880). "[O]n this point something is undoubtedly to be learned from French jurisprudence, which puts it in every man's power to prevent utterly those explorations of his private life which have lately become the fashion with a certain portion of the press and which especially in cases of bereavement or misfortune, give so much pain—often as exquisite pain as mortals know." *Id.* at 736. Warren and Brandeis cited Godkin's work and the influence extends to the replication of certain phraseology.

39. Trib. Civ. Seine, 16.6.1858, D.1858,3,62 (famous actress photographed on her deathbed)

40. C A Paris May 25, 1867.

41. Regarding the evolutionary development in France, see Pierre Kayser, *La protection de la vie privée par le droit* (3d ed. 1995); LINDON, *supra* note 2; FRANCOIS RIGAUX, *LA PROTECTION DE LA VIE PRIVÉE ET DES AUTRES BIENS DE LA PERSONNALITÉ* (1990); Bruggemeier, *supra* note 1; J.Q. Whitman, *The Two Western Cultures of Privacy*, 113 YALE L.J. 1151 (2004).

42. See LINDON, *supra* note 2, at 10-11.

heavily upon the Circular in deriving formula to limit the reach of the privacy right in a democracy. They adopted four key points from the Minister: the right of privacy would not prohibit publishing matters of public or general interest; public figures would necessarily have a smaller sphere of privacy protection than ordinary citizens; the right to privacy would not prohibit publication of privileged matter protected under the laws of defamation; there would be no defense of truth and no requirement of malice in actions for invasion of privacy. These four limitations were borrowed through comparative law research.

Others have noticed that Warren and Brandeis were somewhat vague on important issues. The meaning of privacy, as previously mentioned, was described but never defined. The omission has been criticized⁴³ but clearly it was wise to sidestep such an intractable issue. The different forms of privacy that have evolved in the past 120 years would confirm the difficulty of stating a definition even today, and the inspiring effects that the suggestive phrase “the right to be let alone” had on the imaginations and intuitions of future interpreters cannot be discounted. A different quality in their writing was their flexibility and pragmatism about theoretical matters. For example their arguments were usually at war with the property approach to privacy, but at the same time it was never suggested that the protections of property were wholly inappropriate or should be abandoned. Indeed some of their language suggests that if the common law broadened its conception of intangible property⁴⁴ it might allow privacy interests to be folded in. They were too sensible to discard a theory which already had the respect of a common law audience and could be usefully expanded. Perhaps most crucial in terms of pragmatism is one final point. In the last analysis they abstained altogether from recommending the means by which a right of privacy should be implemented. They offered no doctrinal steps, constructed no new torts, suggested no new catch-holds the common law judge should grasp to instantiate the right of privacy in the common law. Future steps are not even discussed. The solutions were simply entrusted to the judges.

Their *non-discussion* of implementation was in my view an act of pragmatic self-restraint. It reveals authors aware of their limitations, their

43. According to Daniel Solove, their “right to be left alone” provides little guidance about the content of privacy, i.e., the matters in which we should be let alone. SOLOVE, *supra* note 6, at 18.

44. Thus throughout the essay they were careful to distinguish a narrow conception of property that was not capable of protecting privacy interests, as opposed to a wider or enlarged notion (“every form of possession—intangible as well as tangible”) that might englobe such interests. Warren & Brandeis, *supra* note 10, at 193.

audience's conservatism and the unpredictable nature, not to mention the glacial pace, of common law development. It was especially difficult to foresee the roads that English or American judges might actually travel in the future, and they did not presume to draw a roadmap. It was expedient to leave all avenues open. Surely they would not have foreseen the winding road of the past 20 years in England where the courts finally stripped the 'confidential relationship' requirement from the action for breach of confidentiality. Once freed of that limitation, the action seems to have become the principal means of enforcing information privacy in the United Kingdom.⁴⁵ The transformation, however, was unpredictable, long-range and actually it was precipitated by pressures from the European Convention on Human Rights. The authors would have also been hard put to foresee the future path of privacy in the United States, which, as we shall see, began in rejection, recovered in confusion, and later split into four torts.

A. Intervening Years 1890-1970

The Warren and Brandeis article inspired a long line of cases and a prodigious amount of commentary. In looking back over the first seventy years, William Prosser reported that more than 300 cases had been decided, only a few of which rejected the right. A great number of law review articles were also written, many by noted authors, including comparative law studies on the subject.⁴⁶

Ironically the first step in the recognition process was a setback. In the 1902 case of *Roberson v. Rochester Folding Box*⁴⁷ the defendant company published without consent 25,000 copies of an attractive woman's photograph on its flour advertisements, and she sought an injunction against the distribution and damages for her humiliation and suffering. The New York Court of Appeal rejected her claim by a vote of 4-3. The majority opinion dismissed Warren and Brandeis's "clever article" and its "reasoning by analogy", declaring that the so-called right of privacy did not exist. Privacy had no existence apart from the right of

45. See Reid, *supra* note 15, at 289-90; see also Gavin Phillipson, *Transforming Breach of Confidence? Towards a Common Law Right of Privacy Under the Human Rights Act*, 2003 MOD. L. REV. 726.

46. Prosser, *supra* note 11; see H.C. Gutteridge, *The Comparative Law of the Right of Privacy*, 47 LQR 203 (1931); F.P. Walton, *The Comparative Law of the Right of Privacy*, 47 LQR 219 (1931).

47. 171 N.Y. 538, 64 N.E. 442 (1902).

property and to recognize it directly would spawn vast amounts of litigation.⁴⁸

The decision was immediately unpopular and was legislatively overturned shortly thereafter. The New York legislature in the following session made it a misdemeanor and a tort for anyone to use the name, portrait or picture of another for advertising or purposes of trade without written consent.

Two years later, in the leading case of *Pavesich v. New England Life Insurance Co.*, the Supreme Court of Georgia in a unanimous decision rejected the Roberson precedent and gave relief on facts where the New York court had given none. The defendant published plaintiff's picture without permission in a newspaper advertisement, along with the false testimonial that plaintiff had purchased its life insurance. In an exceptionally thorough opinion, the Court placed the foundation of the right of privacy in natural law ("in the instincts of nature") and within the meaning of "liberty" under both the Georgia and United States Constitutions. "It is recognized intuitively, consciousness being the witness that can be called to establish its existence. Any person whose intellect is in a normal condition recognizes at once that as to each individual member of society there are matters private and there are matters public so far as the individual is concerned." Contrary to the approach of Warren and Brandeis who thought the right was a new response to modern conditions and societal needs, the court turned privacy into an immutable "higher law" that had always existed. The relationship between privacy and the right of free expression would be a harmonious coexistence in which "One may be used as a check upon the other; but neither can be lawfully used for the other's destruction."⁴⁹ This case became the leading case in the country, and paved the way for recognition by many others.

48. Justice Gray's dissent closely followed Warren and Brandeis, sometimes incorporating their phrases into his opinion. He noted, "The proposition is, to me, an inconceivable one that these defendants may, unauthorizedly, use the likeness of this young woman upon their advertisement . . . , and that she must submit to the mortifying notoriety, without right to invoke the exercise of the preventive power of a court of equity." His argument at times rested privacy upon property theory, stating that plaintiff should have the same right of property in her own likeness as she has in her literary compositions. "[I]f her face or her portraiture has a value, the value is hers exclusively until the use be granted away to the public."

49. "There is in the publication of one's picture for advertising purposes not the slightest semblance of an expression of an idea, a thought, or an opinion, within the meaning of the constitutional provision [the 1st amendment]. . . ." The same constitutional linkages would be made by subsequent courts. See *Melvin v. Reid*, 297 P. 91 (1931) (privacy linked to inalienable rights of liberty); *Barber v. Time*, 159 S.W.2d 291, 294 (Mo. 1942) (privacy part of the right to liberty and pursuit of happiness).

One of these was the much-discussed case of *Barber v. Time Magazine*.⁵⁰ There the magazine published a story entitled “Starving Glutton” about a woman with an insatiable appetite who had checked into a hospital to receive treatment. Reporters intruded into her room and secured a photograph of her in a hospital gown which was published under the caption “Insatiable-Eater Barber” “She eats for ten”. The Missouri court recognized the privacy right as a part of the inalienable right to liberty and the pursuit of happiness. “Certainly if there is any right of privacy at all, it should include the right to obtain medical treatment at home or in a hospital for an individual personal condition . . . without personal publicity.”⁵¹ In the California case of *Melvin v. Reid*,⁵² a movie was made about a rehabilitated prostitute who had been living a respectable life for a long time. The film dredged up her life history, used her maiden name to identify her and caused her acute humiliation and embarrassment in her unsuspecting social milieu. The California Supreme Court linked the right of privacy to inalienable rights under the California Constitution and found that the movie invaded her privacy.

An important impetus to the acceptance of privacy rights was the backing provided by the First Restatement of Torts of 1939. The Restatement set forth a single provision on the right of privacy, but it had two parts. Privacy was the right to keep private facts out of the public eye and the right to control one’s own likeness.⁵³ Thus conceived, privacy would have to be protected by those two torts alone, and there was no indication that any more torts were gestating, though we know in hindsight that in fact two more were coming. In comments beneath the provision the reporter, Francis Bohlen, made no historical claims that the right emerged out of timeless natural law, as the Pavesich court had done in 1905. Echoing Roscoe Pound, Bohlen wrote “this interest appears only in a comparatively highly developed state of society. It has not been recognized until recently . . .”⁵⁴ Within the Restatement, the provision

50. 159 S.W.2d 291 (1942).

51. *Id.* at 295.

52. 297 P. 91 (1931).

53. This was essentially the scope of the right discussed by Warren and Brandeis. Warren & Brandeis, *supra* note 10. Paragraph 867 of the Restatement of Torts provided: “A person who unreasonably and seriously interferes with another’s interest in not having his affairs known to others or his likeness exhibited to the public is liable to the other.” Five of the six illustrations under the section dealt with the unauthorized publication of a person’s photograph.

54. RESTATEMENT OF TORTS cmt. b at 399 (1939). In discussing the development of personality rights Roscoe Pound, *Interests of Personality*, approvingly quoted Miraglia’s statement: “A man’s rights multiply as his opportunities and capacities develop. The more civilized the nation the richer he is in rights.” Accordingly he argued that privacy is a recent

was classified under a hodgepodge of “miscellaneous rules” including those dealing with interferences to dead bodies, unborn children and the right to vote. Another curiosity is that the provision carried the caption “Interference with Privacy” but the word privacy appeared only in the caption, never in the text itself. Thus matters were couched cautiously, but at least the provision made clear that the right enjoyed an independent existence, and the prestige of the Restatement gave it momentum in American law.

The persistent problem running throughout these years, however, was that privacy was being gradually widened into a portal concept—it was a gateway to various personality rights other than privacy. The phrase “the right to be let alone” had prodigious breadth. It might mean, as Daniel Solove notes, any harmful conduct from a punch in the nose to a peep in the bedroom.⁵⁵ Nothing in this phrase restricted its application to the mischiefs decried by Warren and Brandeis. Interests like controlling one’s name, likeness, one’s life history or one’s past associations could all be addressed in the name of ‘privacy’. Even the emergence of a “right of publicity,” which allowed celebrities the exclusive right to exploit their fame and could be regarded as the antithesis of protecting privacy, was treated by some as a “legitimate offspring” of privacy.⁵⁶ Thus the undefined concept had become a proxy protecting more than privacy could reasonably suggest. All the judges in the cases, from *Pavesich* to *Melvin*, took part in the process of denaturing the word. Seventy years later it fell to William Prosser to restore order.

III. A SECOND MILESTONE: PROSSER’S REFORMULATION OF PRIVACY

Once again a famous law review article brought momentous change to the subject. This milestone was William Prosser’s article “Privacy” published in 1960.⁵⁷ Prosser was undoubtedly the leading U.S. torts scholar of his generation. According to Daniel Solove, he reigned as “the undisputed king of the subject throughout the middle of the twentieth century”. Propelled by his personal influence, his article had such an

demand growing out of the conditions of life in the crowded communities of today. They arise “apart from the law, through the competition of individuals with each other.” Pound, *supra* note 3, at 343, 445.

55. SOLOVE, *supra* note 6.

56. The first leading case was *Haelan Lab Inc. v. Tops Chewing Gum, Inc.*, 202 F.2d 866 (2d Cir. 1953), followed by Melville Nimmer’s *The Right of Publicity*, 19 LAW & CONTEMP. PROBS. 203 (1954). For full background, see Larry Moore, *Regulating Publicity: Does Elvis Want Privacy?*, 5 DEPAUL-LCA J. ART & ENTER. L. 1 (1994/1995).

57. 48 CAL. L. REV. 383 (1960).

impact that some consider it more influential than the seminal work by Warren and Brandeis.⁵⁸

Prosser begins by declaring that the right of privacy had been recognized by the overwhelming majority of the American courts and would probably soon be recognized by more. As of 1960 it stood rejected in only three or four states. Yet, he cautioned, only lately has there been any attempt to inquire what interests are we protecting, and against what conduct. His analysis of three hundred some-odd cases in the books forced him to a somewhat startling conclusion:

What has emerged from the decisions is no simple matter. It is not one tort, but a complex of four. The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff, in the phrase of Judge Cooley, ‘to be let alone.’ Without any attempt to exact definition, these four torts may be described as follows:

1. Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness.

Prosser’s taxonomy was the centerpiece of the article and to this day it remains his central legacy. Much of the article was devoted to a discussion of each tort, mainly to show how the mass of cases really fit into these four piles, and how the actions and the interests protected were disparate and different. Prosser’s achievement here was in one sense a reclassification at a lower level of generality. Peter Birks once observed that Prosser “balkanized” the protection of personality interests when he introduced his four privacies.⁵⁹ This can be taken to mean that he took a general right or interest in privacy and converted it into ‘torticles,’ some of which he admitted were not protecting privacy interests at all and were not related to the original concerns of Brandeis and Warren.⁶⁰ Prosser’s lower-level headings reveal a quintessential common law trait, the tendency to create isolated torts rather than to accept broad subjective

58. See Andrew J. McClung, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 897 (2006).

59. *Harassment and Hubris*, 31 IRISH JURIST 1, 44 (1997).

60. The expression ‘torticles’ is of course borrowed from Bernard Rudden, *Torticles*, 6/7 TUL. EUR. & CIVIL L.F. 105 (1991-1992).

rights. Indeed the broad success his taxonomy enjoys, I submit, reflects the prevalence of this tendency in Anglo-American legal culture.⁶¹

To someone interested in how Prosser (a “mere academic” as they say) achieved such a feat, it should be pointed out that his four torts did not emerge as a sudden brainstorm in and about the year 1960. It had been germinating in Prosser’s mind for many years. As early as 1941, (the date of the first edition of his classic treatise *The Law of Tort*) he had already divided privacy into three discrete actions—intrusions upon solitude, publicity of name or likeness, and commercial appropriation of elements of his personality.⁶² He was three-fourths of the way there, and he alone among the treatise writers was thinking in these terms.⁶³ All that was missing at that point was ‘false light,’ and that idea came to him in time for the Cooley Lectures delivered at the University of Michigan in 1953. He inserted his new four-headed creature almost immediately into the 1955 second edition of his treatise. Thus one could well wonder why the 1960 article, which contained a classification scheme already five years old, has been regarded as a special “moment” in legal development. Neil Richards and Daniel Solove are surely correct in saying the 1960 article actually “broke relatively little new ground.”⁶⁴ Nevertheless the reason for its reputation consists in the article’s special qualities. It contained the first full exposition and reasoned justification of Prosser’s taxonomy. The long format of a law review article allowed him to enlarge upon the subject in ways that the treatise did not afford. He was able through extended discussion to persuade the reader that each tort had distinguishable characteristics, offered different protections, and did not duplicate or conflict with the other three. Suddenly the confusion lifted. Prosser appeared as a paladin who had slain a bewildering mass of cases. In addition the article furnished a long discussion of possible constitutional questions. Here he indicated how the privacy torts were

61. Thus Basil Markesinis observes of English law “that when new needs arise it is better to deal with them by perverting existing institutions rather than by creating new ones.” See *The Familiarity of the Unknown*, in Swadling & Jones (eds.), THE SEARCH FOR PRINCIPLE (1999). Similarly Bernard Rudden observes that “wrongs which might go under general names, . . . are subject to pressure to fragment into more precisely named torts.” Rudden, *supra* note 60, at 128.

62. The breakdown into three categories was first suggested in an article by Gerald Dickler (“[T]he distinctions between these three groups of cases, which may be respectively denominated ‘intrusions,’ ‘disclosures,’ and ‘appropriations,’ have, for the most part, not wormed their way into the minds of courts and writers.”). See Gerald Dickler, *The Right of Privacy: A Proposed Redefinition*, 70 U.S. L. REV. 435, 436 (1936). Judging from Prosser’s very similar language, Dickler’s “trisection” of the cases was of considerable influence.

63. See FOWLER V. HARPER, TREATISE ON THE LAW OF TORTS ¶ 278, at 601-04 (Bobbs Merrill 1933); COOLEY ON TORTS ¶ 190, at 389-92 (Callaghan 1930).

64. Neil Richards & Daniel Solove, *Prosser’s Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887 (2010).

constitutionally consistent with freedom of the press, the public figure doctrine and reporting on matters of public interest.⁶⁵

A. Prosser's Methodology Revisited

Part of Prosser's success was that he made it sound as if the four torts simply emerged from a neutral reading of the cases. To anyone who would read over these same cases, however, Prosser might appear as something rather different than a neutral conduit. That he had normative notions which he superimposed and that he even harbored a certain hostility to this new "right," as Neil Richards and Daniel Solove point out, are in my opinion fair statements.⁶⁶

The tort of "intrusion upon seclusion or solitude" offers a good example of Prosser's way of carving and slicing his torts from a mass of cases. In this instance he seems to have isolated a dramatic circumstance in a range of cases (i.e., *how* and *where* the invasion occurred) and by characterizing this recurring circumstance as 'intrusion' he made it the identifying element of the tort. The intrusion concept clearly required adoption of a spatial concept of privacy. There must be some actual 'thing' or 'area' intruded into, although it did not necessarily have to be owned by the plaintiff.⁶⁷ The necessity of an actual invasion was unique to this one tort; it played no role in the other three. This meant for most cases that protection of property rights served as the invisible tripwire of the tort of intrusion. Prosser admitted as much in saying, "The privacy action which has been allowed in such cases will evidently overlap, to a considerable extent at least, the action for trespass to land or chattels."⁶⁸ This tort had other special features not shared by the other three. Defendant's liability would not depend upon the publication of information acquired in the intrusion; if such publication did result,

65. Richards and Solove say that in functional terms Prosser was as close to a lawmaker as any legislator or judge might have been. He made efforts to reach three audiences. In his role as Reporter on the Restatement of Torts and leading treatise author, he reached the judges and practitioners; as coauthor of a leading casebook, he shaped the views of students in the classroom; and as author of "Privacy," he reached the scholars and teachers with his most cogent account of the subject. *Id.*

66. My own view of Prosser's hostility toward the privacy right was reached at an early stage of this research, before coming across the insightful account by Richards and Solove, *id.* I found myself in basic agreement with their assessment of his role and I am indebted to their article in many respects.

67. It may be sufficient to have an expectation of privacy. *See, e.g.*, Nader v. Gen. Motors, 255 N.E.2d 765 (C.A. N.Y. 1970) (following Ralph Nader into a bank was permissible, but standing in such a way to observe the denomination of bills he withdrew violated his privacy).

68. Prosser, *supra* note 11, at 389-90. As mentioned previously, the action in trespass had been expressly used to protect privacy interests well before Warren and Brandeis's article. Warren & Brandeis, *supra* note 10; *see Note, supra* note 18, at 1895-96.

however, the intrusion could not be justified by the newsworthiness of the information.⁶⁹

Under the heading of intrusion Prosser grouped together such cases as barging into another's home without a warrant, or entering a hotel room or stateroom surreptitiously, or gaining access to private spaces by eavesdropping, secret wiretapping, or peering into windows, or hounding the debtor with telephone calls to the home. To further the impression the tort was distinct and stood on its own feet, he asserted that it was far from the type that Warren and Brandeis had in mind, for (he said) they were merely focused on the evils of publication of private information, not on intrusion upon a plaintiff's seclusion.⁷⁰ Of course here he overlooked what they had actually said. Warren and Brandeis had used the very words 'intrusion' and 'seclusion' in describing the privacy interest and they explicitly adverted to cases involving invasions by trespass or gaining access to information through surreptitious means. It was disingenuous to suggest that they did not appreciate or foresee spatial invasions, given their desire to free the right from the confines of a property-based rationale. Prosser's assertion was basically insensitive to their project. They sought a right of privacy grounded in "inviolate personality,"⁷¹ not to define particular torts or sets of torts, and particularly not a new tort that would ultimately rest upon a property basis.

Prosser's tort of false light provides a second glimpse into his mind and method. False light, the last of the privacies to emerge, was essentially his own invention. It involved 'recharacterizing' a lot of cases that made no mention of the issue. Once again he isolated a factor or characteristic fact in a run of cases—the material published about plaintiff was *false* but not necessarily defamatory—and made this into the linchpin of the tort.⁷² Given the lack of evidence he worked with, the

69. DAN DOBBS, THE LAW OF TORTS ¶ 426, at 1201 (2001).

70. Of course, they would have treated such instances as a *fortiori* invasions and did not need to stress them.

71. "The principle which protects personal writings and all other personal productions, . . . is in reality not the principle of private property, but that of an inviolate personality." Warren & Brandeis, *supra* note 10, at 205. "[N]o basis is discerned upon which the right to restrain publication . . . can be rested, except the right of privacy, as a part of the more general right to the immunity of the person,—the right to one's personality." *Id.* at 207.

72. Perhaps an influence on Prosser was an early article by John H. Wigmore in which he classified various cases of "false attribution". Wigmore's cases included the circulation of poems falsely attributed to Lord Byron, a testimonial for Doan pills falsely attributed to Col. Chinn, and a wife's falsely naming (on a birth certificate) of her husband as father of an adulterous child. Prosser used these examples and regarded all of these as false light cases. See John H. Wigmore, *The Right Against False Attribution of Belief or Utterance*, 4 KENTUCKY L.J. 3 (1916).

wide acceptance of this tort is a great tribute to his personal stature and salesmanship.

As previously mentioned, this tort did not figure in his earliest treatment of privacy in 1941. It surfaced in the mid-1950s in his Cooley lecture, and he described its appearance in the cases as being “rather amorphous”,⁷³ which could almost be an autobiographical reference to his own agency. Partly accounting for the nebulous birth is surely the fact that no one but Prosser himself had ever referred to the cases he had in mind as “false light” cases. A close reading of the cases Prosser cited in support of the new tort reveals no earlier reference or discussion of the concept.⁷⁴ Many of these cases were indeed quite old and, interestingly enough, in prior writings he had classified them differently. For example, Prosser cited the old 1905 Louisiana case of *Itzkovich v. Whitaker*⁷⁵ and now classified it as a false light case. The defendant sheriff was allegedly about to put plaintiff’s photo into the “rogue’s gallery”, though plaintiff was a law-abiding citizen who had not committed a crime. The Supreme Court of Louisiana enjoined the sheriff from doing so, never mentioning false light, but simply emphasizing plaintiff’s right “to be let alone”.⁷⁶ Prosser also prominently relied upon the case of *Hinish v. Meier & Frank* and characterized it a false light case.⁷⁷ The plaintiff was a civil servant prohibited by law from engaging in political activity and his name was signed without his consent or knowledge to a telegram sent to the governor urging the veto of a bill sent to his desk. The Court viewed the defendants’ actions in signing plaintiff’s name as a wrongful appropriation of plaintiff’s personality. It stated: “defendants had appropriated to themselves for their own purposes, without the plaintiff’s consent and against his will, his name, his personality and whatever influence he may have possessed and injected them into a political controversy in which, as far as appears, he had no interest.” The court spoke only of appropriation; Prosser spoke of false light.

73. WILLIAM PROSSER, THE LAW OF TORTS 638 (2d ed. 1955). In the subsequent edition of the treatise (1964 at 837) and in Prosser’s *Privacy* article, *supra* note 11, at 398, he spoke of its debut in the same way: “Over a good many years the principle made a rather nebulous appearance in a line of decisions....”

74. The statement is made on the basis of reviewing the 27 cases cited by Prosser, *supra* note 11, at 398-401.

75. 39 So. 499 (1905). In the first edition of his treatise, WILLIAM PROSSER, THE LAW OF TORTS 1055 (1941), he classified *Itzkovich* in a broadly worded category: “publicity which violates the ordinary decencies given to private information about the plaintiff”.

76. “Everyone who does not violate the law can insist upon being let alone (the right of privacy). In such case the right of privacy is absolute.” 39 So. at 500.

77. 113 P.2d 439 (1941).

The *Hinish* case is one of a number of ‘name appropriation’ cases which Prosser converted into false light cases. The conversion could not be achieved without considerable creativity. In principle the unauthorized use of another’s name and influence for political purposes in *Hinish* was difficult to distinguish from the leading appropriation case in the country, *Pavesich v. New English Life Insurance Co.*⁷⁸ where an insurance company was held liable for the unauthorized use of plaintiff’s name, picture and a spurious testimonial endorsing their product. Yet in his article Prosser classified the two cases differently, calling *Hinish* false light and *Pavesich* appropriation.⁷⁹ Prosser never explained the difference nor why he was now changing his mind. Pavesich’s name, photo and words were clearly appropriated for commercial purposes, but of course at the same time the use of his identity in this way obviously portrayed him in a false light: He was not really insured by the defendant company and had not uttered the words attributed to him in the advertisement. The difficulty with creating an independent tort of false light would seem to be that every appropriation, whether the biographical facts were true or not, would tend to put the plaintiff in a false light. It would create at the very least the false perception in the mind of friends and associates that plaintiff gave his consent, and this alone could be enough to cause feelings of ridicule and humiliation.⁸⁰ Both false light and appropriation result in an alteration of personality, but appropriation was the broader, more inclusive category. One might say that appropriation precedes false light and is more fundamental to liability. The gist of the tort is a nonconsensual taking or alteration of personality. It is immaterial whether the material published is considered true or false. *Pavesich* would have recovered for invasion of privacy even if the defendant’s advertisement were perfectly factual.⁸¹

The point about Prosser’s role in the evolution of the false light category is therefore twofold. First, his creativity was evident in the liberties he took with the cases, retrofitting them to his purposes, and

78. 50 S.E. 68 (1905).

79. Later in the Restatement (Second) of Torts, Prosser may have changed his mind again. *Hinish* is there the basis of an illustration of appropriation, not false light.

80. Thus in *Foster-Milburn v. Chinn*, 120 S.W. 364 (1909), the unauthorized use of plaintiff’s picture and testimonial created the perception that he had authorized the advertisement. As Wigmore noted in discussing the case (at 4), “the plaintiff had not written the letter, nor authorized it, and his friends had ridiculed him by reason of this false publication; moreover, there was a notorious custom of selling such testimonials to medicine-vendors, and this implied possible lack of integrity in the plaintiff.”

81. See DOBBS, *supra* note 69, ¶425, at 1198 (“Since the gist of the tort is the appropriation of the plaintiff’s identity or reputation, or some substantial aspect of it, no element of falsity is required.”).

boldly reading in a rationalization that the judges had not considered, or realized they needed.⁸² Second, similar to the way he devised the intrusion tort, he once again singled out a factual element—the falsity of the material itself—and conceived a tort in terms of it. On the one hand, this tort differed only superficially from the tort of appropriation which inherently took account of the element of false light and, on the other hand, it differed only slightly from the tort of defamation as well as the tort of intentional infliction of emotional distress.⁸³ The niche for the new tort was therefore narrowly situated between closely resembling torts on either side. Dual and overlapping liability would arise easily in many factual situations. This may explain why some have questioned the usefulness of false light, that is, they have asked whether it is “a helpful addition to the armory or merely another piece of baggage that gets in the way.”⁸⁴

B. *Finding Order, Losing Sight of Privacy*

Judge Biggs once described the state of privacy law as “still that of a haystack in a hurricane,”⁸⁵ and Prosser was obviously disturbed by the disarray. His quest was to impose order, to find distinguishing and non-overlapping characteristics for each of his torts, so that none was exactly alike and each might have distinguishable rationale. Yet while the ‘complex’ had an appearance of order,⁸⁶ it did not have intellectual unity. Prosser acknowledged as much in saying that his privacies had *nothing in common* with each other.⁸⁷ Indeed if one looks at the structure closely, there is a complete disconnect between his four torts and the set of

82. See *Kerby v. Hal Roach Studios*, 197 P.2d 577 (1942) (spurious erotic note signed with plaintiff’s name sent to 1000 men as advertising for a movie, causing plaintiff to receive unwanted telephone calls and visitors, and feelings of disgrace); *Peay v. Curtis Pub. Co.*, 78 F. Supp. 305 (D.C. 1948); *Donoghue v. Warner Bros. Pictures*, 194 F.2d 6 (10th Cir. 1952).

83. DOBBS, *supra* note 69, ¶ 428, at 1209.

84. *Id.*

85. Quoted in Prosser, *supra* note 11, at 407.

86. Thus this account of the operating elements:

Taking them in order—intrusion, disclosure, false light, and appropriation—the first and second require the invasion of something secret, secluded or private pertaining to the plaintiff; the third and fourth do not. The second and third depend upon publicity, while the first does not, nor does the fourth, although it usually involves it. The third requires falsity or fiction; the other three do not. The fourth involves use for the defendant’s advantage, which is not true of the rest.

PROSSER ON TORTS 843 (3d ed. 1964).

87. Prosser, *supra* note 11, at 389 (“The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are *tied together by the common name, but otherwise have almost nothing in common* except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley, ‘to be let alone.’”).

privacy interests which was supposedly at its core. This disconnect was never so apparent in Prosser's earliest writings. It really became clear, however, when he became explicit about the underlying interests that each tort protected.⁸⁸ For example, the tort of appropriation of name and likeness was, as already stated, one of the core concerns of Warren and Brandeis ("circulating portraits"). The old 1904 New York statute and the Restatement of 1939 expressly included protections against unauthorized appropriations. Prosser's description of the protected interest, however, completely contradicted that provenance. "The interest protected," he said, "is not so much mental as a proprietary one, in the exclusive use of the plaintiff's name and likeness as an aspect of his identity." This was actually a throwback to the forced and fictional theory of having a property interest in one's own name and identity. It rejects Warren and Brandeis's personality analysis⁸⁹ and reverts to the language of the 19th century English chancellors.⁹⁰ Something similar befell the tort of 'disclosure' when Prosser revealed the underlying protected interest. Prosser now said its purpose was to protect the interests of reputation because it is "in reality an extension of defamation into the field of publications that do not fall within the narrow limits of the old torts, with the elimination of the defense of truth." Here again he differed from Warren and Brandeis who thought that disclosure of private facts is a wrong to "inviolate personality". Reputational interests in their view related more to man's external relations to the community rather than protecting his inner needs and feelings. Coming to false light, Prosser said the interest protected is "clearly that of reputation." In every

88. The change in his interest analysis between 1955 and 1960 is palpable. In the second edition of his treatise he wrote "all three of these torts are primarily concerned with the protection of a mental interest, and that they are only a phase of the larger problem of the protection of peace of mind against unreasonable disturbance." PROSSER ON TORTS, *supra* note 86, at 639 (2d ed. 1955). By 1960, however, his view was that only the intrusion tort rested upon a mental element. The disclosure tort and false light protected reputational interests, while appropriation protected property interests.

89. See Richards & Solove, *supra* note 64.

90. One reason for Prosser's insistence on the proprietary theory is that he was committed to incorporating "right of publicity" cases in the same category with appropriation cases. The publicity right cases, however, had by then gained acceptance as a form of property with a distinct interest. Nimmer, *supra* note 56. Prosser's refusal to distinguish between the two kinds of appropriation interests (one wishing to prevent publicity, the other wishing to profit from it) may have driven him into the arms of the property theory. Ironically, if he had created a fifth tort covering invasion of publicity rights, he might have resisted that conclusion. Jonathan Kahn writes: "The early association of appropriation with such intangible, non-commensurable attributes of the self as dignity and the integrity of one's persona seems to have been lost or at least misplaced as property-based conceptions . . . come to the fore." Jonathan Kahn, *Bringing Dignity Back to Light: Publicity Rights and the Eclipse of the Tort of Appropriation of Identity*, 17 CARDZO ARTIST & ENT. L.J. 213 (1999).

instance, then, the protected interest for Prosser lay in pre-privacy causes of action, not in privacy itself. For that reason it would not be wrong to think of him as standing first in line among “reductionist” writers.⁹¹

Edward Bloustein, Prosser’s most incisive critic, immediately saw the dismantling of the Warren and Brandeis edifice, observing that after Prosser’s intervention there is no “new tort,” just new ways of committing “old torts”.⁹²

But why did Prosser regress to the older protected interests? This cannot be known because Prosser did not tell us how or why he selected one interest over another. One possibility is that it came about by sorting the cases into piles while using an older tort as a template (for example using *trespass* for ‘intrusion’ and *libel* for false light), and then attributing to the new tort the characteristic interest associated with the old. But all we know in the final analysis is that Prosser assigned and attributed ‘interests’ that were *pre-privacy* interests. Privacy itself, the ostensible *casus belli*, was an interest lost in the process.

C. The Four Privacies Enter American Common Law

The Restatement (Second) of Torts adopted Prosser’s four privacies in 1979. Using the prerogatives and powers of a Reporter, Prosser created a new chapter for the subject running to 28 pages (¶ 652(A-J) in which he essentially transplanted his entire taxonomy. A general principle of privacy was stated in ¶ 652A(1): “One who invades the privacy of another is subject to liability for resulting harm to the interests of the other.” The next section filled the space with the four torts, using terms nearly identical to Prosser’s original formulation.⁹³ At this point and for this purpose, he was the most important lawgiver in the United States. The comments stated that these four are the forms which have

91. According to Daniel Solove, *supra* note 6, at 37, reductionists are theorists who argue that “privacy is reducible to other conceptions and rights.” Solove regards Judith Thomson as the most prominent proponent of this view. See Judith Jarvis Thomson, *The Right to Privacy*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272 (F.D. Shoeman ed., 1984).

92. Edward Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 NYU L. REV. 962, 965 (1964). He concluded that “the much vaunted and discussed right of privacy is reduced to a mere shell of what it has pretended to be.” If Prosser’s analysis is accepted, “the social value or interest we call privacy is not an independent one, but is only a composite of the value our society places on protecting mental tranquility, reputation and intangible forms of property.” *Id.* at 966.

93. RESTATEMENT (SECOND) OF TORTS ¶ 652A(2) (1979):

- (a) Unreasonable intrusion upon the seclusion of another
- (b) Appropriation of the other’s name or likeness
- (c) Unreasonable publicity given to the other’s private life
- (d) Publicity that unreasonably places the other in a false light before the public.

crystallized thus far, and others may still appear. But in fact there have been no new privacy torts since Prosser's death. The state courts followed his lead with relatively few exceptions. About forty-five states have adopted one or more of the privacy torts, nearly always following the Restatement definitions.⁹⁴ Even the rather controversial 'false light' tort is recognized in thirty states.⁹⁵

The comments also contained special notes about constitutional questions. The comments about the disclosure tort (Publicity Given to Private Life) said:

It has not been established with certainty that liability of this nature is consistent with the free-speech and free-press provisions of the First Amendment. . . . Since 1964, with the decision of *New York Times v. Sullivan* . . . the Supreme Court has held that the first Amendment has placed a number of substantial restrictions on actions involving false and defamatory publications.

Here the Restaters anticipated a certain amount of constitutional restructuring. To be sure it had always been recognized that privacy rights were subject to constitutional limits, but as Richards and Solove point out, the prior discussions were generally conducted "within the confines of tort law."⁹⁶ Scholars and judges sought the proper balance in the abstract and without the benefit of specific directions and minimum standards from the Supreme Court. That was in the day when tort lawsuits were considered private actions not attributable to the state and not subject to First Amendment scrutiny.⁹⁷ That picture changed in 1964 with *New York Times v. Sullivan*. Before long the new scienter requirements which shielded the press from defamation actions were extended to the tort of false light.⁹⁸

94. See McClung, *supra* note 58, at 897-98, for a comprehensive listing of the cases.

95. Nine states have expressly rejected it; eleven have yet to rule. Ohio was the 30th state to recognize false light, according to the opinion in *Welling v. Weinfeld*, 866 N.E.2d 1051 (Ohio 2007). See also Jessica Long, *Let False Light Flicker On: An Argument in Support of States Adopting a False Light Invasion of Privacy Tort*, www.jesslong.com/upload/falselight_.doc.

96. Richards & Solove, *supra* note 64, at 14.

97. In Richards' and Solove's phrasing, "Before then, tort law treated First Amendment interests . . . not as superseding considerations but as endogenous interests that were balanced in the crafting of legal rules." *Id.*

98. *Time v. Hill*, 385 U.S. 374 (1967) (actual malice standard applied to tort of false light—plaintiff must show defendant either knowingly or recklessly made a false statement without regard for the truth). The 'intrusion' tort may implicate First Amendment considerations as well. See the pending Supreme Court case of *Snyder v. Phelps*, argued October 6, 2010, involving protesters using a deceased marine's funeral as an occasion to object to homosexuality in the military. Adam Liptak, *Justices Take Up Funeral-Protest Case*, N.Y. TIMES, Oct. 7, 2010, at A17.

The most directly impacted action, however, may be the disclosure tort. Here the general question arises whether the truthfulness of the matter disclosed should be a complete defense, or whether truth, as Warren and Brandeis thought, is irrelevant to the question of liability. In *Cox Broadcasting Co. v. Cohn*⁹⁹ the Supreme Court held that the public disclosure of a rape victim's true name by the press was not actionable as an invasion of her privacy, at least not when her name was already published in official records and the information itself was of public interest. The ruling is a challenge to the very idea that truthful revelations of private facts are actionable under state common law.¹⁰⁰ If the disclosure tort is constitutionally hemmed in by two criteria (newsworthiness and prior recordation), there is almost no remaining space for its operation.¹⁰¹ Indeed Novak and Rotunda go so far as to say that "The state should always recognize that truth is a defense in a defamation or right of privacy action—*unless* the defendant publishes confidential information that he himself has stolen."¹⁰² If that were to emerge as the Supreme Court's position, and thus far it is difficult to predict, the disclosure tort might entirely disappear.

IV. THE THIRD MILESTONE: THE CONSTITUTIONAL TRANSFORMATION OF LIBERTY INTO PRIVACY

According to eminent authority, there is a certain paradox within the right of privacy. "It is revered by those who live within civil society as a means of repudiating the claims that civil society would make of them. It is a right that has meaning only within the social environment from which it would provide some degree of escape."¹⁰³ It is nothing less than "society's limiting principle."¹⁰⁴

Starting in the 1960s, the Supreme Court jurisprudence began to transform the privacy concept well into a different set of individual freedoms. As Justice Stevens described the old and new senses of the term, privacy entails on the one hand an individual interest in "avoiding

99. 420 U.S. 469 (1975).

100. The Cox holding was reinforced in *Florida Star v. B.J.F.*, 491 U.S. 524 (1989) (no liability for publishing a rape victim's name obtained from police report); *Landmark Commc'ns Inc. v. Virginia*, 435 U.S. 829 (1978) (no liability for publishing truthful information regarding confidential proceedings of judicial inquiry board); *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97 (1979) (no liability for publishing lawfully obtained name of a juvenile delinquent).

101. Diane Zimmermann, *Requiem for a Heavyweight*, 68 CORNELL L.J. 291 (1983); McClung, *supra* note 58. On newsworthiness and public interest, see *Haynes v. Alfred Knopf*, 8 F.3d 1222 (7th Cir. 1993).

102. JOHN NOVAK & RONALD ROTUNDA, CONSTITUTIONAL LAW ¶ 16.36 (8th ed. 2010).

103. LAWRENCE TRIBE, AMERICAN CONSTITUTIONAL LAW ¶ 15-1, at 1302 (2d ed. 1988).

104. *Id.*

disclosure of personal matters" but on the other hand an "interest in independence in making certain kinds of important decisions."¹⁰⁵ His second category referred to a kind of decisional privacy, a sphere of personal autonomy in which the individual has a right to make fundamental personal decisions free from governmental interference.¹⁰⁶ The sphere included the freedom to marry, the freedom to procreate and rear children, the freedom to move about freely, and so forth. The newly minted category was no longer referring to a sphere of repose and sanctuary under the common law (the privacy of the social personality) which other members of society could not enter without permission. Whereas the emphasis in that sphere was upon the humiliated feelings of the individual, as a constitutional freedom it was upon his power to choose and control his world. This autonomy was not essentially about the individual's power to control the circulation of information about himself. It related to a capacity to project one's self forward in society, to assert her destiny and identity in the world, not merely the freedom to withdraw from it or control the publication of private information. Moreover, invasion of this constitutional right was not by the same invader. The focus was no longer the actions of the press, the gossip columnist or the trespasser, but rather the intrusions of legislatures and government agents. The Constitution protects vertically (freedom from *governmental* interference) rather than horizontally, and thus privacy in the decisional sense was not designed to deflect invasions by private actors. Finally there was another basic difference. This right of privacy was a nationwide guarantee. It was no longer a state-by-state question of tort law.

Fittingly, it was Justice Louis Brandeis who helped supply the hyphen between the older and the newer senses of the right in the case of *Olmstead v. United States*. The case involved the Fourth Amendment, considered the oldest constitutional right to privacy, which protects citizens against unreasonable searches and seizures. Defendants' telephones were wiretapped by government agents from the outside street wires leading to his telephone. Evidence of a criminal conspiracy was thereby gathered without any physical trespass to office or home. The majority of the court found this presented no violation of the Fourth Amendment because there was no literal entry, seizure or searching of defendants' property. Justice Brandeis in dissent, however, saw this

105. Whalen v. Roe, 429 U.S. 589, 599-600 (1977).

106. See Comment, *A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision*, 64 CAL. L. REV. 1447 (1976).

nontrespassory wiretap as an invasion of privacy and a violation of the Fourth Amendment.

The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. . . . They conferred, *as against the government*, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever, the means employed, must be deemed a violation of the Fourth Amendment.¹⁰⁷

The *Olmstead* decision, however, was later overruled in *Katz v. United States* (1967) where the Court announced that the Fourth Amendment protects people, not places, and greatly relied upon Justice Brandeis's view.¹⁰⁸

The first case explicitly to find a constitutional right to privacy was *Griswold v. Connecticut*,¹⁰⁹ where Justice Douglas famously found “zones of privacy” emanating from the First, Third, Fourth, Fifth and Ninth amendments to the Constitution. In striking down a state law banning the use of contraceptives by married couples, the Court said it violated a fundamental right to *marital privacy* which could be found in the “penumbras” of these guarantees.¹¹⁰ Justice Douglas asked, “Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship.” The Court referred to marital privacy as a right “older than the Bill of Rights—older than our political parties, older than our school system.”¹¹¹

Subsequent decisions showed that this fundamental right included various forms of freedom of choice in relation to an individual’s life, for example, the decision to marry,¹¹² to bear children,¹¹³ to maintain custody,¹¹⁴ to live as an extended family under one roof,¹¹⁵ and to exercise

107. 277 U.S. 438, 478 (1928) (emphasis added).

108. 389 U.S. 347 (1967) (the Fourth Amendment protects people not places).

109. 381 U.S. 479 (1965). Earlier, in *Poe v. Ullmann*, 367 U.S. 497 (1961), Justice Harlan had articulated the concept of marital privacy in his dissenting opinion.

110. The penumbral approach by Justice Douglas has been characterized as an attempt to avoid the appearance of using the discredited Lochner approach. It has not been repeated in subsequent decisions. Erwin Chemerinsky considers it “ultimately a due process analysis” in any event. ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES ¶ 10.3.2 (Aspen 2006).

111. *Id.* at 486.

112. *Boddie v. Connecticut*, 401 U.S. 371 (1971); *Loving v. Virginia*, 388 U.S. 1 (1967); *Zablocki v. Redhail*, 434 U.S. 374 (1978).

113. *Roe v. Wade*, 410 U.S. 113 (1973); *Carey v. Population Servs. Int’l*, 431 U.S. 678 (1977).

114. *Santofsky v. Kramer*, 455 U.S. 746 (1982).

choices in child rearing.¹¹⁶ The precise clauses of the Constitution under which these cases were decided (the Equal Protection Clause, the Due Process Clause or the penumbras of certain provisions) were less important for present purposes than the Court's acknowledgment that a fundamental interest in autonomy and privacy was at stake. The most famous ruling was *Roe v. Wade* where the Court held that a woman's right to choose to terminate her pregnancy was part of her right of privacy.¹¹⁷ The freedom to choose a sexual lifestyle was upheld in *Lawrence v. Texas* where a statute banning sodomy between persons of the same sex was struck down.¹¹⁸ Whether an individual has a right to choose death over life, for example by refusing medical treatment or by committing suicide, has been considered by the court but there is no definitive ruling.¹¹⁹ It is not out of the question that this may one day be recognized as a part of the right of privacy. Personal choices concerning hair length and clothes would also seem to involve one's autonomy and physical personality, but regulations mandating uniform dress and appearance regulations for school children and the police have usually been upheld.¹²⁰ Nevertheless for one eminent judge such regulations were an unacceptable effort to submerge and standardize individuality:

Hair . . . for centuries has been one aspect of the manner in which we hold ourselves out to the rest of the world. . . . A person shorn of the freedom to vary the length and style of his hair is forced against his will to hold himself out symbolically as a person holding ideas contrary, perhaps, to ideas he holds most dear. Forced dress, including forced hair style, humiliates the unwilling complier, forces him to submerge his individuality in the 'undistracting' mass, and in general, smacks of the exaltation of organization over member, unit over component, and state over individual.¹²¹

115. *Moore v. City of Cleveland*, 431 U.S. 494 (1977).

116. *Pierce v. Soc'y of Sisters*, 268 U.S. 510 (1925); *Meyer v. Nebraska*, 262 U.S. 390 (1923). These older decisions are usually regarded as privacy cases.

117. 410 U.S. 113 (1973) (the right of privacy in 14th Amendment is "broad enough" to encompass a woman's decision to terminate her pregnancy); *see also* *Planned Parenthood v. Casey*, 505 U.S. 833 (1992); *Stenberg v. Earhart*, 530 U.S. 914 (2000).

118. 539 U.S. 558 (2003), *overruling* *Bowers v. Hardwick*, 478 U.S. 186 (1986).

119. *Cruzan v. Dir., Mo. Dep't of Health*, 497 U.S. 261 (1990).

120. *TRIBE*, *supra* note 103, ¶ 15-15, at 1384-89.

121. *Karr v. Schmidt*, 460 F.2d 609, 621 (5th Cir 1972) (Wisdom, J., dissenting).

V. CONCLUSION

The subject of personality rights is sometimes presented as if it were exclusively a civilian concept¹²² or possibly a civilian invention which emerged during the nineteenth century, inspired in large part by Revolutionary thinking, the French jurisprudence and German writers like Kant and von Gierke. The study of privacy in the United States, however, shows that personality rights can have an entirely different kind of history and taxonomy than on the Continent. Many personality rights are recognized in the United States as if they were aspects of privacy. The subsumption of these rights under privacy was accomplished by the growth of a somewhat vague and undisciplined category. Today it is the gateway to protections against unauthorized use of an individual's name, likeness, publicity rights, confidences, compositions, and life history; it is also the expression of a zone of autonomous decisionmaking relating to marriage, abortion, childbearing and childrearing. Lying at the intersection between private and constitutional law, it illustrates an interactive process whereby private law meanings influence constitutional meanings, and the counterthrust of the constitution defines the limits of the private law.

122. Adrian Popovici, *Personality Rights—A Civil Law Concept*, 50 LOY. L. REV. 349 (2004).

W. A. PARENT

Privacy, Morality, and the Law

I. THE DEFINITION OF PRIVACY

Defining privacy requires a familiarity with its ordinary usage, of course, but this is not enough since our common ways of talking and using language are riddled with inconsistencies, ambiguities, and paradoxes. What we need is a definition which is by and large consistent with ordinary language, so that capable speakers of English will not be genuinely surprised that the term "privacy" should be defined in this way, but which also enables us to talk consistently, clearly, and precisely about the family of concepts to which privacy belongs. Moreover the definition must not usurp or encroach upon the basic meanings and functions of the other concepts within this family. Drawing useful and legitimate distinctions between different values is the best antidote to exploitation and evisceration of the concept of privacy.

Let me first state and then elaborate on my definition. Privacy is the condition of not having undocumented personal knowledge about one possessed by others. A person's privacy is diminished exactly to the degree that others possess this kind of knowledge about him. I want to stress that what I am defining is the condition of privacy, not the right to privacy. I will talk about the latter shortly. My definition is new, and I believe it to be superior to all of the other conceptions that have been proffered when measured against the desiderata of conceptual analysis above.

A full explication of the personal knowledge definition requires that we clarify the concept of personal information. My suggestion is that it be understood to consist of *facts* about a person¹ which most individuals

1. The spreading of falsehoods or purely subjective opinions about a person does not constitute an invasion of his privacy. It is condemnable in the language of libel or slander.

in a given society at a given time do not want widely known about themselves. They may not be concerned that a few close friends, relatives, or professional associates know these facts, but they would be very much concerned if the information passed beyond this limited circle. In contemporary America facts about a person's sexual preferences, drinking or drug habits, income, the state of his or her marriage and health belong to the class of personal information. Ten years from now some of these facts may be a part of everyday conversation; if so their disclosure would not diminish individual privacy.

This account of personal information, which makes it a function of existing cultural norms and social practices, needs to be broadened a bit to accommodate a particular and unusual class of cases of the following sort. Most of us don't care if our height, say, is widely known. But there are a few persons who are extremely sensitive about their height (or weight or voice pitch).² They might take extreme measures to ensure that other people not find it out. For such individuals height is a very personal matter. Were someone to find it out by ingenious snooping we should not hesitate to talk about an invasion of privacy.

Let us, then, say that personal information consists of facts which most persons in a given society choose not to reveal about themselves (except to close friends, family, . . .) or of facts about which a particular individual is acutely sensitive and which he therefore does not choose to reveal about himself, even though most people don't care if these same facts are widely known about themselves.

Here we can question the status of information belonging to the public record, that is, information to be found in newspapers, court proceedings, and other official documents open to public inspection. (We might discover, for example, that Jones and Smith were arrested many years ago for engaging in homosexual activities.) Should such information be excluded from the category of personal information? The answer is that it should not. There is, after all, nothing extraordinary about public documents containing some very personal information. I will hereafter refer to personal facts belonging to the public record as documented.

My definition of privacy excludes knowledge of documented personal information. I do this for a simple reason. Suppose that A is browsing

2. I know a recently divorced man who doesn't want anyone to know the fact. He and his former wife still live together, so it is possible for him to conceal their marital status from most everyone.

through some old newspapers and happens to see B's name in a story about child prodigies who unaccountably failed to succeed as adults. B had become an obsessive gambler and an alcoholic. Should we accuse A of invading B's privacy? No. An affirmative answer blurs the distinction between the public and the private. What belongs to the public domain cannot without glaring paradox be called private; consequently it should not be incorporated within our concept of privacy.

But, someone might object, A might decide to turn the information about B's gambling and drinking problems over to a reporter who then publishes it in a popular news magazine. Isn't B's privacy diminished by this occurrence?³ No. I would certainly say that his reputation might well suffer from it. And I would also say that the publication is a form of gratuitous exploitation. But to challenge it as an invasion of privacy is not at all reasonable since the information revealed was publicly available and could have been found out by anyone, without resort to snooping or prying. In this crucial respect, the story about B no more diminished his privacy than would have disclosures about his property interests, say, or about any other facts concerning him that belonged to the public domain.

I hasten to add that a person does lose a measure of privacy at the time when personal information about him first becomes a part of the public record, since the information was until that time undocumented. It is also important not to confuse documented facts as I define them here with facts about individuals which are kept on file for special purposes but which are not available for public consumption, for example, health records. Publication of the latter does imperil privacy; for this reason special precautions are usually taken to ensure that the information does not become public property.

I believe the personal knowledge definition isolates the conceptual one of privacy, its distinctive and unique meaning. It does not appropriate ideas which properly belong to other concepts. Unfortunately the three most popular definitions do just this, confusing privacy with quite different values.

1. *Privacy consists of being let alone.* Warren and Brandeis were the first to advocate this broad definition.⁴ Brandeis movingly appealed to

3. I owe this example, as well as other useful comments and suggestions, to an Editor of *Philosophy & Public Affairs*.

4. Samuel Warren and Louis Brandeis, "The Right to Privacy," *The Harvard Law Review*, 4 (1980): 205-07.

it again in his celebrated dissent to the U.S. Supreme Court's majority ruling in *Olmstead v. U.S.*⁵ Objecting to the Court's view that telephone wiretapping does not constitute a search and seizure, Brandeis delivered an impassioned defense of every citizens' right to be let alone, which he called our most cherished entitlement. Several other former U.S. Supreme Court Justices have endorsed this conception of privacy, among them Douglas, Fortas, and Stewart.⁶ And a number of distinguished law professors have done likewise.⁷

What proponents of the Brandeis definition fail to see is that there are innumerable ways of failing to let a person alone which have nothing to do with his privacy. Suppose, for instance, that A clubs B on the head or repeatedly insults him. We should describe and evaluate such actions by appeal to concepts like force, violence, and harassment. Nothing in the way of analytical clarity and justificatory power is lost if the concept of privacy is limited, as I have suggested that it be, to cases involving the acquisition of undocumented personal knowledge. Inflationary conceptions of privacy invite muddled reasoning.

2. *Privacy consists of a form of autonomy or control over significant personal matters.* "If the right to privacy means anything, it is the right of the individual, married or single, to be free from unwarranted government invasion into matters so fundamentally affecting a person as the decision whether to bear or beget a child."⁸ With these words, from the Supreme Court case of *Eisenstadt v. Baird*, Mr. Justice Brennan expresses a second influential theory of privacy.

Indeed, definitions of privacy in terms of control dominate the literature. Perhaps the most favored among them equates privacy with the

5. *Olmstead v. U.S.*, 277 U.S. 438 (1928): 475–76.

6. See William Douglas, *The Rights of the People* (Westport, CT: Greenwood Press, 1958). See Fortas's decision in *Time v. Hill*, 385 U.S. 374 (1967): 412; and in *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974): 412–13. See Stewart's decision in *Katz v. U.S.*, 389 U.S. 347 (1967): 350; and in *Whalen v. Roe*, 429 U.S. 589 (1977): 608.

7. For example, Edward Bloustein, in "Group Privacy: The Right to Huddle," from his *Individual and Group Privacy* (New Brunswick, NJ: Transaction Books, 1978), pp. 123–86; Paul Freund, in "Privacy: One Concept or Many?" ed. J. Pennock and J. Chapman, *Nomos XIII: Privacy* (New York: Atherton Press, 1971), pp. 182–98; Henry Paul Monaghan, "Of 'Liberty' and 'Property,'" *Cornell Law Review* 62 (1977): pp. 405–14; and Richard Posner, *The Economics of Justice* (Cambridge, MA: Harvard University Press, 1981), p. 123.

8. *Eisenstadt v. Baird*, 405 U.S. 438 (1972): 453.

control over personal information about oneself. Fried, Wasserstrom, Gross, and Beardsley all adopt it or a close variation of it.⁹ Other lawyers and philosophers, including Van Den Haag, Altman, and Parker,¹⁰ identify privacy with control over access to oneself, or in Parker's words, "control over when and by whom the various parts of us can be sensed by others."

All of these definitions should be jettisoned. To see why, consider the example of a person who voluntarily divulges all sorts of intimate, personal, and undocumented information about himself to a friend. She is doubtless exercising control, in a paradigm sense of the term, over personal information about herself as well as over (cognitive) access to herself. But we would not and should not say that in doing so she is preserving or protecting her privacy. On the contrary, she is voluntarily relinquishing much of her privacy. People can and do choose to give up privacy for many reasons. An adequate conception of privacy must allow for this fact. Control definitions do not.¹¹

I believe the voluntary disclosure counterexample is symptomatic of a deep confusion underlying the thesis that privacy is a form of control. It is a conceptual confusion, the mistaking of privacy for a part of liberty. The defining idea of liberty is the absence of external restraints or coercion. A person who is behind bars or locked in a room or physically pinned to the ground is unfree¹² to do many things. Similarly a person who is prohibited by law from making certain choices should be described as having been denied the liberty or freedom to make them. The loss of liberty in these cases takes the form of a deprivation of autonomy. Hence

9. Charles Fried, *An Anatomy of Values* (Cambridge, MA: Harvard University Press, 1970), chap. 9, p. 141; Richard Wasserstrom, "Privacy: Some Assumptions and Arguments," in *Philosophical Law*, ed. Richard Brunaugh (Westport, CT: Greenwood Press, 1979), pp. 148–67; Hyman Gross, "Privacy and Autonomy," *Nomos XIII*, p. 170; Elizabeth Beardsley, "Privacy, Autonomy, and Selective Disclosure," *Nomos XIII*, p. 65.

10. Ernest Van Den Haag, "On Privacy," *Nomos XIII*, p. 147ff.; Irwin Altman, "Privacy—A Conceptual Analysis," *Environment and Behavior* 8 (1976): 8; and "Privacy Regulation: Culturally Universal or Culturally Specific?" *The Journal of Social Issues* 33 (1977): 67; Richard Parker, "A Definition of Privacy," *Rutgers Law Review* 27 (1974): 280.

11. Proponents of a control definition might respond by saying that they are really interested in identifying *the right to privacy* with the right to control personal information about or access to ourselves. But then they should have said so explicitly instead of formulating their contention in terms of privacy alone. And even if they had done so their position would still be confused, since the right to choose is an integral aspect of the right to liberty, not the right to privacy.

12. Here I use "unfree" to mean "lacking liberty." My concern is not with the metaphysical notion of free will.

we can meaningfully say that the right to liberty embraces in part the right of persons to make fundamentally important choices about their lives and therewith to exercise significant control over different aspects of their behavior. It is clearly distinguishable from the right to privacy, which condemns the unwarranted acquisition of undocumented personal knowledge.¹³

3. *Privacy is the limitation on access to the self.* This definition, defended by Garrett and Gavison¹⁴ among others, has the virtue of separating privacy from liberty. But it still is unsatisfactory. If we understand "access" to mean something like "physical proximity," then the difficulty becomes that there are other viable concepts which much more precisely describe what is at stake by limiting such access. Among these concepts I would include personal property, solitude, and peace. If, on the other hand, "access" is interpreted as referring to the acquisition of personal knowledge, we're still faced with a seemingly intractable counterexample. A taps B's phone and overhears many of her conversations, including some of a very intimate nature. Official restraints have been imposed on A's snooping, though. He must obtain permission from a judge before listening in on B. This case shows that limitation of cognitive access does not imply privacy.

A response sympathetic with the Garrett-Gavison conception to the above criticism might suggest that they really meant to identify privacy with certain kinds of limitations on access to the self. But why then didn't they say this, and why didn't they tell us what relevant limitations they had in mind?

Let us suppose that privacy is thought to consist of certain normal limitations on cognitive access to the self. Should we accept this conception? I think not, since it confuses privacy with the existential conditions that are necessary for its realization. To achieve happiness I must have some good luck, but this doesn't mean that happiness is good luck.

13. I do not mean to ascribe to proponents of control definitions the view that every interference with liberty is by that very fact an infringement to privacy. I do mean to criticize them for failing to recognize that interferences with personal choice or control, taken by themselves and with no consideration given to undocumented personal knowledge that might be acquired from them, are not appropriately described or persuasively condemned in the language of privacy.

14. Roland Garrett, "The Nature of Privacy," *Philosophy Today* 18 (1974): 264; and Ruth Gavison, "Privacy and the Limits of the Law," *Yale Law Journal* 89 (1980): 428.

Similarly, if I am to enjoy privacy there have to be limitations on cognitive access to me, but these limitations are not themselves privacy. Rather privacy is what they safeguard.

PRIVACY 2020

10 Privacy Risks and 10 Privacy Enhancing Technologies to Watch in the Next Decade

DATA PRIVACY DAY 2020



Jules Polonetsky | CEO, Future of Privacy Forum
Elizabeth Renieris | Founder, hackylawyerER

INTRODUCTION

Data is the lifeblood of modern organizations. Data collection and uses impact society and human interactions in unprecedented ways and will only become more important in the 2020s. The processing of personal data is increasingly recognized as a human right and quickly being extensively regulated to ensure lawful, fair, and transparent practices.

The existing data ecosystem is complex and the influence of data-intensive technologies is rapidly extending. Policymakers, privacy professionals, executives, and civil society must understand the basics of these technologies in order to assess how existing and proposed policies, systems, and laws will address the risks and benefits of emerging technologies, and to support appropriate guidance for the implementation of new digital products and services.

The Future of Privacy Forum has identified ten technologies or trends that will likely create increasingly complex data protection challenges over the next decade. We also highlight ten developments that can enhance privacy and, consequently, other rights – reasons to be optimistic that organizations will be better able to manage data responsibly. Some of these technologies are already in general use, some will soon be widely deployed, and others are nascent.

Technological advances are creating data protection challenges. But ultimately, managing key issues will continue to require trained people at the center of organizations to bring the human dimension to review products and services, to assess bias, to demand fairness, and to manage the systems and tools that can handle data protection at scale.

TEN PRIVACY RISKS TO WATCH IN THE 2020s

Innovations in Tech Linked to Human Bodies, Health, and Social Interaction

1. **Biometric Scanning** – The increasing use of biometric-based recognition represents a general shift away from graphical user interfaces (GUIs) that depend on a keyboard or screen to biometric-enabled UIs such as Voice User Interfaces (VUIs) and other Natural User Interfaces (NUIs). Biometric scanning is based on machine learning systems, techniques, and algorithms that collect unique biometric features to identify individuals and infer attributes about them. Examples include voiceprints (used in voice recognition technology and voice-activated devices), facial scans (used in facial characterization and facial recognition technology), behavior and gestures (recognition based on bodily movements), physiological (such as flushed skin, or heart rate), and potentially genetic information.¹ Biometric interfaces will require organizations to assess how to apply traditional data protection and privacy principles in the absence of a screen or manual device input. Development of this technology will further blur the divide between law enforcement and consumer privacy concerns. Organizations building, selling, and deploying biometric scanning technologies should also consider fairness and justice concerns, such as training data shortfalls related to lack of diversity that can create or perpetuate systemic bias. In addition, security applications relying on biometric scanning systems may need to consider their accuracy as the market for “biometric camouflage” makeup, clothing, and wearables grows.
2. **Real World Evidence** – Real World Evidence (RWE) makes use of data from mobile devices, electronic health records, claims and billing activity and other patient generated data to assess

¹ See 2019 Tech Trends Report (12th ed.), Future Today Institute, at 97-98 (hereinafter “FTI Trends Report”).

the safety and effectiveness of drugs or medical devices.² To the extent that many of the data sets collected may not be protected by HIPAA, regulators and organizations will need to ensure legal protections and enforceable commitments to protect this data and assure individuals of beneficial uses.

3. **Social Credit and Reputation Scoring Systems** – These systems derive rankings about individuals from algorithms built on behavioral data gleaned from social media and web posts, including the quantity and quality of an individual's online presence, an individual's contacts, social ties and interactions, personality attributes as extracted from their online posts, and more.³ While consumers may be aware that sharing economy services use scoring algorithms within their apps to rate both providers and users, social credit and reputation scoring systems collect data from sources that span services and platforms, sweeping in a much broader array of unexpected information about an individual. Moreover, these analyses and scores may impact a person's ability to access certain products and services, or affect pricing. The inferences and recommendations regarding the ranked or scored individual have privacy implications for both them and their contacts and will need careful scrutiny.⁴ But these automated individual assessments will likely have consequences on other rights as well. Without the sort of transparency and oversight provided by traditional credit scoring laws and regulations such as the Fair Credit Reporting Act (FCRA), fairness, algorithmic transparency, and accountability are core challenges for organizations designing and deploying these new, alternative scoring systems.
4. **Internet of Bodies and Brain-Machine Interfaces** – Just as the Internet of Things (IoT) refers to a network of devices connected to or powered by the Internet, the Internet of Bodies (IoB) refers to a network of medical and biometric devices that attach to or are inside of our bodies and connected to the Internet.⁵ While people have largely accepted wearables like smart watches, IoB devices may also include devices such as smart contact lenses, Bluetooth-enabled "smart pills," and WiFi-enabled pacemakers.⁶ These more intimate devices raise a number of legal, ethical, and security challenges, including who should have access to the data they generate, how to mitigate the risks of malicious hacking, how to apply existing legal frameworks, and who is liable for vulnerabilities, malfunctions, or breaches. Even when looking to regulatory guidance, authority over some IoB devices between the Food and Drug

² Statement from FDA Commissioner Scott Gottlieb, M.D., on FDA's new strategic framework to advance use of real-world evidence to support development of drugs and biologics, FDA Statement (Dec. 6, 2018), <https://www.fda.gov/news-events/press-announcements/statement-fda-commissioner-scott-gottlieb-md-fdas-new-strategic-framework-advance-use-real-world>.

³ Niran Geslevich Packin & Yafit Lev-Aretz, *On Social Credit and the Right to Be Unnetworked*, Colum. Bus. L. Rev., 2016.

⁴ See id.

⁵ Andrea M. Matwyshyn, *The 'Internet of Bodies' Is Here. Are Courts and Regulators Ready?* via The Wall Street Journal (Nov. 12, 2018), <https://www.wsj.com/articles/the-internet-of-bodies-is-here-are-courts-and-regulators-ready-1542039566>.

⁶ See id.

Administration, the Consumer Product Safety Commission, Federal Trade Commission, or Health and Human Services (HHS) may be dependent on specific use contexts.⁷

A brain-machine interface (BMI), also known as brain-computer interface (BCI), mind-machine interface (MMI), direct neural interface (DNI), or human-machine interface (HMI), is a computer interface that can connect humans and machines by allowing people to communicate and control devices with their thoughts alone.⁸ These interfaces have promising medical applications for victims of stroke and paralysis, as well as commercial applications, such as their use in autonomous vehicles as brain-to-vehicle interfaces. They raise significant privacy and security concerns, such as the risk of “brain-jacking” whereby malicious actors illicitly access wireless devices to change the implant settings, to access sensitive information about the patient, or to use the implant as a pivot point into hospital systems via less secure connections.⁹ Commercial actors may also seek to pursue “neuromarketing” by using data from fMRIs, EEGs, eye tracking technology, and facial analysis to offer products, set prices, and improve ads.¹⁰ In the future, companies may learn how to more effectively create market segments based on individuals with similar characteristics and proclivities. Environmental cues such as particular smell, or lighting controls might be provided to influence propensities, even while sleeping.¹¹ These kinds of activities pose ethical as well as privacy and security challenges and will require standards and guidance to protect the privacy of neural information and data derived from it.

Innovations in Infrastructure

5. **Automation and (Collaborative) Robotics** – While advances in software-enabled automation, digital home assistants, and simple robotics are generally available, increasingly sophisticated robots and AI-based systems are imminent. Robots that share data and code and perform computations remotely by accessing cloud-based data or systems promise greater efficiency and additional opportunities for services and collective learning across systems and platforms. An example of such “cloud robots” are semi-autonomous vehicles that access remote data for maps, real-time traffic conditions, etc.¹² Further in the future, collaborative robots or “cobots” could help other robots work more collaboratively and increase the effectiveness of robot-robot or robot-human partnerships. In such cases, it will become more challenging for existing legal frameworks to address data that is cogenerated by humans and machines, sometimes in different groups or locations. Security will be a significant concern, and organizations using cloud bots, for example, should ensure that the data is encrypted both at rest and in transit, and may also want to consider using advanced techniques such as homomorphic encryption

⁷ See *id.*

⁸ FTI Trends Report, *supra* note 1, at 173.

⁹ Kimberley Mok, *How Brain Hacking Computer Interfaces Could Expose us to Hacking and Manipulation*, The New Stack (Dec. 25., 2017), <https://thenewstack.io/brain-computer-interfaces-expose-us-hacking-manipulation/>.

¹⁰ Jonathan Pugh, *Brainjacking in deep brain stimulation and autonomy*, Ethics and Information Technology (September 2018, Volume 20, Issue 3, p. 219) <https://link.springer.com/article/10.1007/s10676-018-9466-4/>.

¹¹ Eban Harrell, *Neuromarketing: What You Need to Know*, Harvard Business Review (January 23, 2019), <https://hbr.org/2019/01/neuromarketing-what-you-need-to-know/>.

¹² FTI Trends Report, *supra* note 1, at 166.

to further reduce the risks posed by these models. In addition to the security risks associated with the increasing incorporation of robots and automated systems into homes and offices, there are heightened risks to privacy with the ability to collect and store more intimate information. In public, or semi-public/commercial environments informing individuals and providing controls will need creative designs beyond what is provided today. In many cases, awareness of the presence and role of AI-based systems will be critical to meeting individuals' expectations.

6. **Location Services and Proximity Tracking** – Precise location data is available via the location services on mobile devices which leverage GPS, WiFi and cell tower proximity.¹³ Bluetooth beacons further assist services that determine proximity, as do the Bluetooth signals emitted by a wide range of devices such as wearables. Devices broadcast their MAC addresses, and venues can use Mobile Location Analytics (MLA) to detect how devices are moving within a space, and to identify repeat visitors. Soon, “5G” wireless technology will accommodate an exponentially expanding and complex data ecosystem by providing additional bandwidth to enable faster speeds, lower latency, and more connectivity. This technology will serve in supporting the technology for digital maps, geographic information systems (GIS), and more.¹⁴ 5G signals have a shorter range, and so they require more numerous, smaller cellular towers, including indoors, potentially adding to the availability of location data. As these varied services come online, organizations connecting and communicating with consumers via these technologies will need a plan for complying with location data-related data protection and privacy requirements. Location data can potentially reveal sensitive information about individuals (religious beliefs related to their presence at certain worship venues, health related information revealed by presence at specific clinics etc.), mobility patterns, or aspects related to one's behavior, thus posing risks to privacy and safety.
7. **Smart Communities** – A smart community or smart city generally refers to a city or locality that integrates information communications technologies (ICT) and Internet of Things (IoT) sensors into its traditional infrastructure (e.g. roads, parks, buildings, etc.) with the aim of connecting and enhancing the lives of its citizens and providing responsive environments.¹⁵ The importance and impact of smart cities will increase with the trend towards urbanization, as 70% of the world's population is estimated to live in cities by 2050.¹⁶ Because of the vast amounts of data collection and consolidation possible in these wired cities, there are significant concerns about the risks to individual privacy, particularly with respect to sensitive information, including license plate tracking, facial recognition, government access to rideshare or mobility data, and deployment of a wide range of sensors that capture data in public spaces. Limited individual control and the impact of security breaches could expose people to significant risks. Private organizations participating in smart city projects or providing products and services to municipalities should consider the need for transparency, accountability, and public

¹³ Matthew Kassel, *As 5G Technology Expands, So Do Concerns Over Privacy*, The Wall Street Journal (Feb. 26, 2019), https://www.wsj.com/articles/as-5g-technology-expands-so-do-concerns-over-privacy-11551236460?mod=rss_Technology.

¹⁴ *What 5G Means for Your Business*, Networked World (Apr. 19, 2017), <https://www.networkworld.com/article/3191264/what-5g-means-for-your-business.html>.

¹⁵ FTI Trends Report, *supra note 1*, at 334.

¹⁶ *Powering Fast Forward Thinking*, The AXA 2019 Foresight Trend Book, AXA, at 8, <https://group.axa.com/en/newsroom/publications/2019-foresight-trendbook>.

consultation, as well as administrative and constitutional due process-related concerns.¹⁷ Contracts should clearly determine rights and responsibilities in respect of data collection, processing, storage, demarcate points of contact, and outline how they will give effect to individual rights. Regulators seeking access to mobility data will need to consider data minimization, risks of law enforcement access to data, and re-identification due to breaches or FOIA requests. Communities should develop thorough, transparent data policies that maximize the utility of public data to residents and minimize privacy risks to individuals, while following community developed ethical standards.

Innovations in Computing

8. **Quantum Computing** – Quantum computing applies the laws of quantum physics to systems that process information and solve advanced computational problems.¹⁸ Whereas classical computing uses “bits” holding a single binary value of 0 or 1, quantum computing uses “qubits” that can hold both values at the same time (known as “superposition”) and can be highly correlated (known as “entanglement”).¹⁹ Quantum physics enables computing that is orders of magnitude faster, allowing for more advanced computation and better predictive analysis, with the potential to deliver breakthroughs in scientific and medical research, quantum chemistry, molecular modeling, real-time financial modeling, and advanced supply chain automation, among others. Security experts are worried about the potential ability of quantum computers to defeat modern forms of encryption relied on by existing data protection and data security practices.²⁰ However, quantum computers may also support new methods of encryption that are more secure.²¹ Although quantum computers are unlikely to become mainstream in the near future, enterprises should at least begin to consider how they will protect information and digital assets in their transition to a post-quantum world.
9. **Spatial Computing (Augmented Reality/Virtual Reality)** – Spatial computing is a computing environment that seamlessly maps physical spaces and the people, places, and things inside of them, making digital information feel as though it is both physically present and reactive to the environment.²² It works through a combination of technologies including video and audio sensors, 3D-capture, rendering, algorithms, and mixed-reality wearable displays that track the user’s movements and relay information to the system.²³ For example, smart glasses project light directly into the user’s eye to make it appear as though digital objects exists in the user’s

¹⁷ See Notice of Application, CCLA v Waterfront Toronto (Quayside), <http://ccla.org/cclanewsite/wp-content/uploads/2019/04/Notice-of-Application-CCLA-and-Lester-Brown.pdf>.

¹⁸ *What is Computing?* (Microsoft), <https://www.microsoft.com/en-us/quantum/what-is-quantum-computing>.

¹⁹ Daniel Wellers, *7 Innovations that could Shape the Future of Computing*, World Economic Forum (Sept. 21, 2016), <https://www.weforum.org/agenda/2016/09/7-innovations-that-could-shape-the-future-of-computing>.

²⁰ David Roe, *Quantum Computing Brings Potential and Risks to the Enterprise*, via CMS Wire (Dec. 3, 2018), <https://www.cmswire.com/information-management/quantum-computing-brings-potential-and-risk-to-the-enterprise/>.

²¹ Larry Greenemeier, *How Close are we Really to Building a Quantum Computer?* in Scientific American (May 30, 2018), <https://www.scientificamerican.com/article/how-close-are-we-really-to-building-a-quantum-computer/>.

²² See FTI Trends Report, *supra note 1*, at 363.

²³ Amy Webb, *I Tested Working in a Mixed-Reality Office. It's Closer Than You Think*, via Inc. (WINTER 2018/2019 ISSUE), <https://www.inc.com/magazine/201902/amy-webb/augmented-mixed-reality-virtual-workplace-magic-leap.html>

physical world and surroundings.²⁴ These systems can collect a constant stream of user data, including everything the user sees and hears, as well as information collected and cross-referenced from applications using the system, content the user is watching or participating in, and any third-party apps or services integrated into the user experience. Design decisions regarding which data is stored locally and controls over third party apps will be essential to manage privacy issues.

10. **Distributed Ledger Technology (“Blockchain”)** – A DLT, the most common of which is blockchain, is a record of verified transactions grouped into time-ordered digital entries known as blocks, which are sequenced together and verified by a digital fingerprint known as a hash.²⁵ The “distributed” aspect reflects the fact that the digital record (or ledger) is replicated and stored across a non-centralized network of computers, called nodes. Originally developed to create a monetary exchange system without the middlemen of banks or financial institutions, blockchain technology may be adaptable for commercial implementations, promising to facilitate “trustless” information sharing (that is, between parties that do not know each other) and immutable transaction storage. Although there are not yet any fully developed commercial applications of blockchain outside of cryptocurrency systems, proposed use cases include financial services, supply chain management, and identity management, among others. In addition to significant logistical hurdles around speed, scale, and security, public blockchains are unlikely to be compatible with data protection frameworks, due to the inability to meet requirements for rectification, erasure, and restriction of processing of personal data. Organizations seeking to leverage blockchain technology may want to undertake a privacy impact assessment, consider reducing the amount of personal data tied to the ledger, incorporate the use of advanced cryptographic and anonymization techniques, or include off-chain governance frameworks to give effect to individual rights regarding personal data.²⁶

TEN PRIVACY ENHANCING TECHNOLOGIES TO WATCH IN THE 2020s

Many of the opportunities offered by emerging technologies relate to increased speed, efficiency, productivity, commercial output, and connectivity. To the extent that these benefits rely upon more extensive collection and processing of personal data, they pose data protection and security challenges. Here are ten technological innovations and techniques that may be useful tools to manage privacy risks. At present, few of these are developed enough to be immediately transformative and each has limitations, but all are already having an impact in the market.

Advances in Cryptography

1. **Zero Knowledge Proofs** – Zero knowledge proof (ZKPs) are cryptographic methods by which one party can prove to another party that they know something to be true without conveying

²⁴ FTI Trends Report, *supra note 1*, at 284-285.

²⁵ Dr. Garrick Hileman & Michel Rauchs, *Global Blockchain Benchmarking Study (2017)*, Cambridge Centre for Alternative Finance, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf.

²⁶ We are skeptical that blockchain will have transformative business or social impact, but we include it in this paper because we believe that the drive to test blockchain related strategies will create privacy risks that could be consequential.

any additional information (like how or why the mathematical statement is true). ZKPs can be used in identity verification contexts, for example, to prove that someone is over a certain age without revealing their exact date of birth. ZKPs help with data minimization and data protection and promote privacy by design and default.

2. **Homomorphic Encryption** – Homomorphic encryption is a process that enables privacy-preserving data analysis by allowing some types of analytical functions and computations to be performed on encrypted data without first needing to decrypt the data.²⁷ It may be especially useful in applications that retain encrypted data in cloud storage for central access.
3. **Secure Multi-Party Computation** – Secure multi-party computation (SMPC) is a distributed computing system or technique that provides the ability to compute values of interest from multiple encrypted data sources without any party having to reveal their private data to the others. A common example is secret sharing, whereby data from each party is divided and distributed as random, encrypted “shares” among the parties, and when ultimately combined can provide the desired statistical result.²⁸ Compromising one share is insufficient to expose the remaining data. SMPC holds particular promise for sharing or managing access to sensitive data such as health records, but in some cases may still be vulnerable to revealing inferences about individuals.
4. **Differential Privacy** – Differential privacy (DP) is a rigorous mathematical definition of privacy that quantifies the risk that an individual is included in a data set. It leverages anonymization techniques that involve the addition of statistical “noise” to data sets before calculations are computed and results released. DP can be global or local.²⁹ Global DP is server-side anonymization or de-identification (where trust resides in the service provider); local DP is applied on the client or user’s device. There are now differentially private versions of algorithms in machine learning, game theory and economic mechanism design, statistical estimation, and streaming. Differential privacy works better on larger databases because as the number of individuals in a database grows, the effect of any single individual on a given aggregate statistic diminishes. SMPC and DP are federated learning approaches.

Localization of Processing

5. **Edge computing and Local Processing** – For devices where speed is of the essence or connectivity is not constant, applications, data, and services are increasingly run away from centralized nodes at the end points of a network. Such local processing helps with data minimization by reducing the amount of data that must be collected (accessible) by the service provider, or retained on a centralized service or in cloud storage.

²⁷ See David Wu, University of Virginia Computer Science Department, available at <https://www.cs.virginia.edu/dwu4/fhe-project.html>.

²⁸ See Christopher Sadler, *Protecting Privacy with Secure Multi-Party Computation*, New America (Jan. 11, 2018), <https://www.newamerica.org/oti/blog/protecting-privacy-secure-multi-party-computation/>.

²⁹ Evaluation of Privacy-Preserving Technologies for Machine Learning, Outlier Ventures Research (Nov. 2018), <https://outlierventures.io/research/evaluation-of-privacy-preserving-technologies-for-machine-learning/>.

6. **Device-Level Machine Learning** – New machine learning focused semiconductor components and algorithms — along with the speedy, low-cost local storage and local processing capabilities of edge computing — are allowing tasks that used to require the computing horsepower of the cloud to be done in a more refined and more focused way on edge devices.
7. **Identity Management** – Many identity management solutions under consideration or development leverage a variety of platforms, including distributed ledger technology (described previously), and local processing, that capitalize on device-level machine learning to provide the ability for individuals to verify and certify their identity. This enables people without internet access beyond smartphones or other simple devices to form secure connections, exchange identity-related credentials (such as transcripts or voting records) without going through a centralized intermediary. Verified personal data can be accessed from the user's device and shared via secure, encrypted channels to third parties, with data limited to the basic facts necessary for the relying party (e.g. that the individual is over 21, or does in fact qualify for a specific government service) on an as-needed basis. Depending on the implementation and standards, identity management can create privacy risks or can be deployed to support data minimization and privacy by design and default.

Advances in Artificial Intelligence (AI) & Machine Learning (ML)

8. **“Small Data”** – Small data AI and machine learning systems use significantly less, or even no real data, via techniques such as data augmentation (manipulating existing data sets), transfer learning (importing learnings from a preexisting model), synthetic data sets (see below), and others.³⁰ With small data techniques, the future forms of AI might be able to operate without needing the tremendous amounts of training data currently required for many applications.³¹ This capability can greatly reduce the complexity and privacy risks associated with AI and ML systems.
9. **Synthetic Data Sets** – Synthetic data sets are sets of artificial data created to replicate the patterns and analytic potential of real data about real individuals or events by replicating the important statistical properties of real data.³² They can be created at a vast scale and reduce the need for large training or test data sets, particularly for AI and ML applications, and thus support reduced data sharing or secondary use concerns.
10. **Generative Adversarial Networks** – Generative Adversarial Networks (GANs) are a type of artificial intelligence, in which algorithms are created in pairs (one to “learn,” and the other to “judge”). Used in unsupervised machine learning, two neural networks contest with each other in a framework to produce increasingly better simulations of real data (e.g., creating faces of people, or handwriting). One valuable use: generating synthetic data sets.³³

³⁰ Harsha Angeri, *Small Data & Deep Learning (AI): A Data Reduction Framework*, Medium (Apr. 1, 2018), <https://medium.com/datadriveninvestor/small-data-deep-learning-ai-a-data-reduction-framework-9772c7273992>.

³¹ H. James Wilson, Paul R. Daugherty, Chase Davenport, *The Future of AI Will be About Less Data, Not More*, Harvard Business Review (Jan. 14, 2019), <https://hbr.org/2019/01/the-future-of-ai-will-be-about-less-data-not-more>.

³² Applied AI, *Synthetic Data: An Introduction & 10 Tools*, (June 2018 update), <https://blog.appliedai.com/synthetic-data/>.

³³ Dan Yin and Qing Yang, *GANs Based Density Distribution Privacy-Preservation on Mobility Data*, Security and Communication Networks, vol. 2018, Article ID 9203076, (Dec. 2, 2018), <https://doi.org/10.1155/2018/9203076>.

These tools and resources can potentially help mitigate data protection concerns posed by future technologies. The broader market for compliance tools for privacy and security professionals continues to accelerate and includes a wide range of legal, technical and policy tools and will be the subject of our next report, jointly with the Privacy Tech Alliance. Services that discover, map, and categorize data for organizations, wizards that help manage and complete privacy impact assessments, programs that handle data subject access requests and consent management, and de-identification services are already supporting privacy and security professionals at leading organizations as well as attracting investor interest. Data protection resources entering the market are increasingly central to building systems that allow professionals to manage the challenges that accompany the expanded data collection and the multiplying uses.

SHORT TERM

Browsers, Operating Systems and Platforms - Much of the important digital activity today takes place on top of technology structures operated by a number of leading companies. Access to data is enabled or restricted by decisions those organizations make and the technical or contractual requirements they establish. The last few years have been marked by these platforms implementing a host of restrictions, due to a range of reasons including regulatory pressure, media and consumer backlash due to well publicized scandals such as Cambridge Analytica, and browser and operating system competition. It is notable that as of January 2020, every leading browser has strictly limited or committed to limit most third party cookie tracking, a staple of today's data ecosystem. We expect a continued pivot to privacy as these companies compete in sectors such as cloud, smart city, automotive, education, health, payments and other areas that are highly regulated or where data and trust expectations are not compatible with the broad data sharing of ad tech.

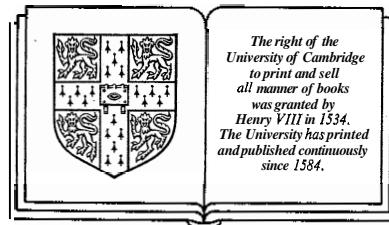
CONCLUSION

The digital world is entering a qualitatively different era, marked by tremendous advances in the kinds and quantity of information and inferences collected and the contexts in which the data is generated and used. Major shifts in user experiences and user interfaces (UX/UI) are adding amazing possibilities, but also adding complexity and challenges. The nature of the data ecosystem is more interactive, more pervasive, and more encompassing, which means that the ex-ante design of products and services, as well as ongoing assessments and calibration, are absolutely essential to enable effective data protection and provide acceptable privacy controls and outcomes for individuals. Organizations should explore and embrace advances in cryptography, evolving data minimization and analysis techniques, and small data/local processing trends to sufficiently mitigate risks. With a focus and strategy for data stewardship, organizations can make careful decisions about the benefits and risks of new technologies, as well as the required safeguards.

*Philosophical Dimensions
of Privacy:
An Anthology*

Edited by
FERDINAND DAVID SCHOEMAN
*Department of Philosophy
University of South Carolina, Columbia*

© Cambridge University Press 1984



CAMBRIDGE UNIVERSITY PRESS

CAMBRIDGE
LONDON NEW YORK NEW ROCHELLE
MELBOURNE SYDNEY

Privacy

[A legal analysis]

WILLIAM L. PROSSER

In the year 1890 Mrs. Samuel D. Warren, a young matron of Boston, which is a large city in Massachusetts, held at her home a series of social entertainments on an elaborate scale. She was the daughter of Senator Bayard of Delaware, and her husband was a wealthy young paper manufacturer, who only the year before had given up the practice of law to devote himself to an inherited business. Socially Mrs. Warren was among the élite; and the newspapers of Boston, and in particular the *Saturday Evening Gazette*, which specialized in "blue blood" items, covered her parties in highly personal and embarrassing detail. It was the era of "yellow journalism," when the press had begun to resort to excesses in the way of prying that have become more or less commonplace today;¹ and Boston was perhaps, of all of the cities in the country, the one in which a lady and a gentleman kept their names and their personal affairs out of the papers. The matter came to a head when the newspapers had a field day on the occasion of the wedding of a daughter, and Mr. Warren became annoyed.² It was an annoyance for which the press, the advertisers and the entertainment industry of America were to pay dearly over the next seventy years.

Mr. Warren turned to his recent law partner, Louis D. Brandeis, who was destined not to be unknown to history. The result was a noted article, *The Right to Privacy*,³ in the *Harvard Law Review*, upon which the two men collaborated. It has come to be regarded as the outstanding example of the influence of legal periodicals upon the American law. In the Harvard Law School class of 1877 the two authors had stood respectively second and first, and both of them were gifted with scholarship, imagination, and ability. Internal evidences of style, and the probabilities of the situation, suggest that the writing, and perhaps most of the research, was done by Brandeis; but

it was undoubtedly a joint effort, to which both men contributed their ideas.

Piecing together old decisions in which relief had been afforded on the basis of defamation, or the invasion of some property right,⁴ or a breach of confidence or an implied contract,⁵ the article concluded that such cases were in reality based upon a broader principle which was entitled to separate recognition. This principle they called the right to privacy; and they contended that the growing abuses of the press made a remedy upon such a distinct ground essential to the protection of private individuals against the outrageous and unjustifiable infliction of mental distress. This was the first of a long line of law review discussions of the right of privacy,⁶ of which this is to be yet one more. With very few exceptions,⁷ the writers have agreed, expressly or tacitly, with Warren and Brandeis.

The article had little immediate effect upon the law. The first case to allow recovery upon the independent basis of the right of privacy was an unreported decision⁸ of a New York trial judge, when an actress very scandalously, for those days, appeared upon the stage in tights, and the defendant snapped her picture from a box, and was enjoined from publishing it. This was followed by three reported cases in New York,⁹ and one in a federal court in Massachusetts,¹⁰ in which the courts appeared to be quite ready to accept the principle. Progress was brought to an abrupt halt, however, when the Michigan court flatly rejected the whole idea, in a case¹¹ where a brand of cigars was named after a deceased public figure. In 1902 the question reached the Court of Appeals of New York, in the case of *Roberson v. Rochester Folding Box Co.*¹² in which the defendant made use of the picture of a pulchritudinous young lady without her consent to advertise flour, along with the legend, "The Flour of the Family." One might think that the feebleness of the pun might have been enough in itself to predispose the court in favor of recovery; but in a four-to-three decision, over a most vigorous dissent, it rejected Warren and Brandeis and declared that the right of privacy did not exist, and that the plaintiff was entitled to no protection whatever against such conduct. The reasons offered were the lack of precedent, the purely mental character of the injury, the "vast amount of litigation" that might be expected to ensue, the difficulty of drawing any line between public and private figures, and the fear of undue restriction of the freedom of the press.

The immediate result of the *Roberson* case was a storm of public disapproval, which led one of the concurring judges to take the un-

precedented step of publishing a law review article in defense of the decision.¹³ In consequence the next New York Legislature enacted a statute¹⁴ making it both a misdemeanor and a tort to make use of the name, portrait or picture of any person for "advertising purposes or for the purposes of trade" without his written consent. This act remains the law of New York, where there have been upwards of a hundred decisions dealing with it. Except as the statute itself limits the extent of the right, the New York decisions are quite consistent with the common law as it has been worked out in other states, and they are customarily cited in privacy cases throughout the country.

Three years later the supreme court of Georgia had much the same question presented in *Pavesich v. New England Life Insurance Co.*,¹⁵ when the defendant's insurance advertising made use of the plaintiff's name and picture, as well as a spurious testimonial from him. With the example of New York before it, the Georgia court in turn rejected the *Roberson* case, accepted the views of Warren and **Brandeis**, and recognized the existence of a distinct right of privacy. This became the leading case.

For the next thirty years there was a continued dispute as to whether the right of privacy existed at all, as the courts elected to follow the *Roberson* or the *Pavesich* case. Along in the thirties, with the benediction of the *Restatement of Torts*,¹⁶ the tide set in strongly in favor of recognition, and the rejecting decisions began to be overruled. At the present time the right of privacy, in one form or another, is declared to exist by the overwhelming majority of the American courts. It is recognized in Alabama,¹⁷ Alaska,¹⁸ Arizona,¹⁹ California,²⁰ Connecticut,²¹ the District of Columbia,²² Florida,²³ Georgia,²⁴ Illinois,²⁵ Indiana,²⁶ Iowa,²⁷ Kansas,²⁸ Kentucky,²⁹ Louisiana,³⁰ Michigan,³¹ Mississippi,³² Missouri,³³ Montana,³⁴ Nevada,³⁵ New Jersey,³⁶ North Carolina,³⁷ Ohio,³⁸ Oregon,³⁹ Pennsylvania,⁴⁰ South Carolina,⁴¹ Tennessee,⁴² and West Virginia.⁴³ It will in all probability be recognized in Delaware⁴⁴ and Maryland,⁴⁵ where a federal and a lower court have accepted it; and also in Arkansas,⁴⁶ Colorado,⁴⁷ Massachusetts,⁴⁸ Minnesota,⁴⁹ and Washington,⁵⁰ where the courts at least have refrained from holding that it does not exist, but the decisions have gone off on other grounds. It is recognized in a limited form by the New York statute,⁵¹ and by similar acts adopted in Oklahoma,⁵² Utah,⁵³ and Virginia.⁵⁴

At the time of writing the right of privacy stands rejected only by a 1909 decision in Rhode Island,⁵⁵ and by more recent ones in Nebraska,⁵⁶ Texas,⁵⁷ and Wisconsin,⁵⁸ which have said that any change

in the old common law must be for the legislature, and which have not gone without criticism.

In nearly every jurisdiction the first decisions were understandably preoccupied with the question whether the right of privacy existed at all, and gave little or no consideration to what it would amount to if it did. It is only in recent years, and largely through the legal writers, that there has been any attempt to inquire what interests are we protecting, and against what conduct. Today, with something over three hundred cases in the books, the holes in the jigsaw puzzle have been largely filled in, and some rather definite conclusions are possible.

What has emerged from the decisions is no simple matter. It is not one tort, but a complex of four. The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley,⁵⁹ "to be let alone." Without any attempt to exact definition, these four torts may be described as follows:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

It should be obvious at once that these four types of invasion may be subject, in some respects at least, to different rules; and that when what is said as to any one of them is carried over to another, it may not be at all applicable, and confusion may follow.

The four may be considered in detail, in order.

I. Intrusion

Warren and **Brandeis**, who were concerned with the evils of publication, do not appear to have had in mind any such thing as intrusion upon the plaintiff's seclusion or solitude. Nine years before their article was published there had been a Michigan case⁶⁰ in which a young man had intruded upon a woman in childbirth, and the court,

invalidating her consent because of fraud, had allowed recovery without specifying the ground, which may have been trespass or battery. In retrospect, at least, this was a privacy case. Others have followed, in which the defendant has been held liable for intruding into the plaintiff's home,⁶¹ his hotel room,⁶² and a woman's stateroom on a steamboat,⁶³ and for an illegal search of her shopping bag in a store.⁶⁴ The privacy action which has been allowed in such cases will evidently overlap, to a considerable extent at least, the action for trespass to land or chattels.

The principle was, however, soon carried beyond such physical intrusion. It was extended to eavesdropping upon private conversations by means of wire tapping⁶⁵ and microphones,⁶⁶ and there are three decisions,⁶⁷ the last of them aided by a Louisiana criminal statute, which have applied the same principle to peering into the windows of a home. The supreme court of Ohio, which seems to be virtually alone among our courts in refusing to recognize the independent tort of the intentional infliction of mental distress by outrageous conduct,⁶⁸ has accomplished the same result⁶⁹ under the name of privacy, in a case where a creditor hounded the debtor for a considerable length of time with telephone calls at his home and his place of employment.⁷⁰ The tort has been found in the case of unauthorized prying into the plaintiff's bank account,⁷¹ and the same principle has been used to invalidate a blanket subpoena duces tecum requiring the production of all of his books and documents,⁷² and an illegal compulsory blood test.⁷³

It is clear, however, that there must be something in the nature of prying or intrusion, and mere noises which disturb a church congregation,⁷⁴ or bad manners, harsh names and insulting gestures in public,⁷⁵ have been held not to be enough. It is also clear that the intrusion must be something which would be offensive or objectionable to a reasonable man, and that there is no tort when the landlord stops by on Sunday morning to ask for the rent.⁷⁶

It is clear also that the thing into which there is prying or intrusion must be, and be entitled to be, private. The plaintiff has no right to complain when his pre-trial testimony is recorded,⁷⁷ or when the police, acting within their powers, take his photograph, fingerprints or measurements,⁷⁸ or when there is inspection and public disclosure of corporate records which he is required by law to keep and make available.⁷⁹ On the public street, or in any other public place, the plaintiff has no right to be alone, and it is no invasion of his privacy to do no more than follow him about.⁸⁰ Neither is it such an invasion to take his photograph in such a place,⁸¹ since this amounts to nothing

more than making a record, not differing essentially from a full written description, of a public sight which any one present would be free to see. On the other hand, when he is confined to a hospital bed,⁸² and in all probability when he is merely in the seclusion of his home, the making of a photograph without his consent is an invasion of a private right, of which he is entitled to complain.

It appears obvious that the interest protected by this branch of the tort is primarily a mental one. It has been useful chiefly to fill in the gaps left by trespass, nuisance, the intentional infliction of mental distress, and whatever remedies there may be for the invasion of constitutional rights.

II. Public disclosure of private facts

Because of its background of personal annoyance from the press, the article of Warren and Brandeis was primarily concerned with the second form of the tort, which consists of public disclosure of embarrassing private facts about the plaintiff. Actually this was rather slow to appear in the decisions. Although there were earlier instances in which other elements were involved, its first real separate application was in a Kentucky case⁸⁴ in 1927, in which the defendant put up a notice in the window of his garage announcing to the world that the defendant owed him money and would not pay it. But the decision which has become the leading case, largely because of its spectacular facts, is *Melvin v. Reid*,⁸⁵ in California in 1931. The plaintiff, whose original name was Gabrielle Darley, had been a prostitute, and the defendant in a sensational murder trial. After her acquittal she had abandoned her life of shame, become rehabilitated, married a man named Melvin, and in a manner reminiscent of the plays of Arthur Wing Pinero, had led a life of rectitude in respectable society, among friends and associates who were unaware of her earlier career. Seven years afterward the defendant made and exhibited a motion picture, called "The Red Kimono," which enacted the true story, used the name of Gabrielle Darley, and ruined her new life by revealing her past to the world and her friends. Relying in part upon a vague constitutional provision that all men have the inalienable right of "pursuing and obtaining happiness," which has since disappeared from the California cases, the court held that this was an actionable invasion of her right of privacy.

Other decisions have followed, involving the use of the plaintiff's name in a radio dramatization of a robbery of which he was the victim,⁸⁶ and publicity given to his debts,⁸⁷ to medical pictures of his

anatomy,⁸⁸ and to embarrassing details of a woman's masculine characteristics, her domineering tendencies, her habits of profanity, and incidents of her personal conduct toward her friends and neighbors.⁸⁹ Some limits, at least, of this branch of the right of privacy appear to be fairly well marked out, as follows:

First, the disclosure of the private facts must be a public disclosure, and not a private one. There must be, in other words, publicity. It is an invasion of the right to publish in a newspaper that the plaintiff does not pay his debts,⁹⁰ or to post a notice to that effect in a window on the public street⁹¹ or cry it aloud in the highway,⁹² but, except for one decision of a lower Georgia court which was reversed on other grounds,⁹³ it has been agreed that it is no invasion to communicate that fact to the plaintiff's employer,⁹⁴ or to any other individual, or even to a small group,⁹⁵ unless there is some breach of contract, trust or confidential relation which will afford an independent basis for relief.⁹⁶ Warren and Brandeis⁹⁷ thought that the publication would have to be written or printed unless special damage could be shown; and there have been decisions⁹⁸ that the action will not lie for oral publicity; but the growth of radio alone has been enough to make this obsolete,⁹⁹ and there now can be little doubt that writing is not required.¹⁰⁰

Second, the facts disclosed to the public must be private facts, and not public ones. Certainly no one can complain when publicity is given to information about him which he himself leaves open to the public eye, such as the appearance of the house in which he lives, or to the business in which he is engaged. Thus it has been held that a public school teacher has no action for a compulsory disclosure of her war work and other outside activities.¹⁰¹

Here two troublesome questions arise. One is whether any individual, by appearing upon the public highway or in any other public place, makes his appearance public, so that any one may take and publish a picture of him as he is at the time. What if an utterly obscure citizen, reeling along drunk on the main street, is snapped by an enterprising reporter, and the picture given to the world? Is his privacy invaded? The cases have been much involved with the privilege of reporting news and other matters of public interest,¹⁰² and for that reason cannot be regarded as very conclusive; but the answer appears to be that it is not. The decisions indicate that anything visible in a public place may be recorded and given circulation by means of a photograph, to the same extent as by a written description,¹⁰³ since this amounts to nothing more than giving publicity to what is already

public and what any one present would be free to see.¹⁰⁴ Outstanding is the California case¹⁰⁵ in which the plaintiff, photographed while embracing his wife in the market place, was held to have no action when the picture was published. It has been contended¹⁰⁶ that when an individual is thus singled out from the public scene, and undue attention is focused upon him, there is an invasion of his private rights; and there is one New York decision to that effect.¹⁰⁷ It was, however, later explained upon the basis of the introduction of an element of fiction into the accompanying narrative.¹⁰⁸

On the other hand, it seems clear that when a picture is taken surreptitiously, or over the plaintiff's objection, in a private place,¹⁰⁹ or one already made is stolen,¹¹⁰ or obtained by bribery or other inducement of breach of trust,¹¹¹ the plaintiff's appearance which is thus made public is at the time still a private thing, and there is an invasion of a privaté right, for which an action will lie.

The other question is as to the effect of the fact that the matter made public is already one of public record. If the record is a confidential one, not open to public inspection, as in the case of income tax returns,¹¹² it is not public, and there can be no doubt that there is an invasion of privacy. But it has been held that no one is entitled to complain when there is publication of his recorded date of birth or his marriage,¹¹³ or his military service record;¹¹⁴ and the same must certainly be true of his admission to the bar or to the practice of medicine, or the fact that he is driving a taxicab. The difficult question is as to the effect of lapse of time, and the extent to which forgotten records, as for example of a criminal conviction, may be dredged up in after years and given more general publicity. As in the case of news,¹¹⁵ with which the problem may be inextricably interwoven, it has been held that the memory of the events covered by the record, such as a criminal trial,¹¹⁶ can be revived as still a matter of legitimate public interest. But there is the leading case of *Melvin v. Reid*,¹¹⁷ which held that the unnecessary use of the plaintiff's name, and the revelation of her history to new friends and associates, introduced an element which was in itself a transgression of her right of privacy. The answer may be that the existence of a public record is a factor of a good deal of importance, which will normally prevent the matter from being private, but that under some special circumstances it is not necessarily conclusive.

Third, the matter made public must be one which would be offensive and objectionable to a reasonable man of ordinary sensibilities.¹¹⁸ All of us, to some extent, lead lives exposed to the public gaze or to

the public inquiry, and complete privacy does not exist in this world except for the eremite in the desert. Any one who is not a hermit must expect the more or less casual observation of his neighbors and the passing public as to what he is and does, and some reporting of his daily activities. The ordinary reasonable man does not take offense at mention in a newspaper of the fact that he has returned from a visit, or gone camping in the woods, or that he has given a party at his house for his friends; and very probably Mr. Warren would never have had any action for the reports of his daughter's wedding. The law of privacy is not intended for the protection of any shrinking soul who is abnormally sensitive about such publicity.¹¹⁹ It is quite a different matter when the details of sexual relations are spread before the public gaze,¹²⁰ or there is highly personal portrayal of his intimate private characteristics or conduct.¹²¹

Here the outstanding case is *Sidis v. F-R Publishing Corporation*.¹²² The plaintiff, William James Sidis, had been an infant prodigy, who had graduated from Harvard at sixteen, and at the age of eleven had lectured to eminent mathematicians on the fourth dimension. When he arrived at adolescence he underwent some unusual psychological change, which brought about a complete revulsion toward mathematics, and toward the publicity he had received. He disappeared, led an obscure life as a bookkeeper, and occupied himself in collecting street car transfers, and studying the lore of the Okamakammessett Indians. The *New Yorker* magazine sought him out, and published a not unsympathetic account of his career, revealing his present whereabouts and activities. The effect upon Sidis was devastating, and the article unquestionably contributed to his early death. The case involved the privilege of reporting on matters of public interest;¹²³ but the decision that there was no cause of action rested upon the ground that there was nothing in the article which would be objectionable to any normal person. When this case is compared with *Melvin v. Reid*,¹²⁴ with its revelation of the past of a prostitute and a murder defendant, what emerges is something in the nature of a "mores" test,¹²⁵ by which there will be liability only for publicity given to those things which the customs and ordinary views of the community will not tolerate.

This branch of the tort is evidently something quite distinct from intrusion. The interest protected is that of reputation, with the same overtones of mental distress that are present in libel and slander. It is in reality an extension of defamation, into the field of publications that do not fall within the narrow limits of the old torts, with the elimination of the defense of truth.¹²⁶ As such, it has no doubt gone

far to remedy the deficiencies of the defamation actions, hampered as they are by technical rules inherited from ancient and long forgotten jurisdictional conflicts, and to provide a remedy for a few real and serious wrongs that were not previously actionable.

III. False light in the public eye

The third form of invasion of privacy, which Warren and Brandeis again do not appear to have had in mind at all, consists of publicity that places the plaintiff in a false light in the public eye. It seems to have made its first appearance in 1816, when Lord Byron succeeded in enjoining the circulation of a spurious and inferior poem attributed to his pen.¹²⁷ The principle frequently, over a good many years, has made a rather nebulous appearance in a line of decisions¹²⁸ in which falsity or fiction has been held to defeat the privilege of reporting news and other matters of public interest, or of giving further publicity to already public figures. It is only in late years that it has begun to receive any independent recognition of its own.

One form in which it occasionally appears, as in Byron's case, is that of publicity falsely attributing to the plaintiff some opinion or utterance.¹²⁹ A good illustration of this might be the fictitious testimonial used in advertising,¹³⁰ or the Oregon case¹³¹ in which the name of the plaintiff was signed to a telegram to the governor urging political action which it would have been illegal for him, as a state employee, to advocate. More typical are spurious books and articles, or ideas expressed in them, which purport to emanate from the plaintiff.¹³² In the same category are the unauthorized use of his name as a candidate for office,¹³³ or to advertise for witnesses of an accident,¹³⁴ or the entry of an actor, without his consent, in a popularity contest of an embarrassing kind.¹³⁵

Another form in which this branch of the tort frequently has made its appearance is the use of the plaintiff's picture to illustrate a book or an article with which he has no reasonable connection. As remains to be seen,¹³⁶ public interest may justify a use for appropriate and pertinent illustration. But when the face of some quite innocent and unrelated citizen is employed to ornament an article on the cheating propensities of taxi drivers,¹³⁷ the negligence of children,¹³⁸ profane love,¹³⁹ "man hungry" women,¹⁴⁰ juvenile delinquents,¹⁴¹ or the peddling of narcotics,¹⁴² there is an obvious innuendo that the article applies to him, which places him in a false light before the public, and which is actionable.

Still another form in which the tort occurs is the inclusion of the plaintiff's name, photograph and fingerprints in a public "rogues' gallery" of convicted criminals, when he has not in fact been convicted of any crime.¹⁴³ Although the police are clearly privileged to make such a record in the first instance, and to use it for any legitimate purpose pending trial,¹⁴⁴ or even after conviction,¹⁴⁵ the element of false publicity in the inclusion among the convicted goes beyond the privilege.

The false light need not necessarily be a defamatory one, although it very often is,¹⁴⁶ and a defamation action will also lie. It seems clear, however, that it must be something that would be objectionable to the ordinary reasonable man under the circumstances, and that, as in the case of disclosure,¹⁴⁷ the hypersensitive individual will not be protected.¹⁴⁸ Thus minor and unimportant errors in an otherwise accurate biography, as to dates and place, and incidents of no significance, do not entitle the subject of the book to recover,¹⁴⁹ nor does the erroneous description of the plaintiff as a cigarette girl when an inquiring photographer interviews her on the street.¹⁵⁰ Again, in all probability, something of a "mores" test must be applied.

The false light cases obviously differ from those of intrusion, or disclosure of private facts. The interest protected is clearly that of reputation, with the same overtones of mental distress as in defamation. There is a resemblance to disclosure; but the two differ in that one involves truth and the other lies, one private or secret facts and the other invention. Both require publicity. There has been a good deal of overlapping of defamation in the false light cases, and apparently either action, or both, will very often lie. The privacy cases do go considerably beyond the narrow limits of defamation, and no doubt have succeeded in affording a needed remedy in a good many instances not covered by the other tort.

It is here, however, that one disposed to alarm might express the greatest concern over where privacy may be going. The question may well be raised, and apparently still is unanswered, whether this branch of the tort is not capable of swallowing up and engulfing the whole law of public defamation; and whether there is any false libel printed, for example, in a newspaper, which cannot be redressed upon the alternative ground. If that turns out to be the case, it may well be asked, what of the numerous restrictions and limitations which have hedged defamation about for many years, in the interest of freedom of the press and the discouragement of trivial and extortionate claims? Are they of so little consequence that they may be circumvented in so casual and cavalier a fashion?

IV. Appropriation

There is little indication that Warren and Brandeis intended to direct their article at the fourth branch of the tort, the exploitation of attributes of the plaintiff's identity. The first decision¹⁵¹ had relied upon breach of an implied contract, where a photographer who had taken the plaintiff's picture proceeded to put it on sale; and this is still one basis upon which liability continues to be found.¹⁵² By reason of its early appearance in the *Roberson case*,¹⁵³ and the resulting New York statute,¹⁵⁴ this form of invasion has bulked rather large in the law of privacy. It consists of the appropriation, for the defendant's benefit or advantage, of the plaintiff's name or likeness.¹⁵⁵ Thus in New York, as well as in many other states, there are a great many decisions in which the plaintiff has recovered when his name¹⁵⁶ or picture,¹⁵⁷ or other likeness,¹⁵⁸ has been used without his consent to advertise the defendant's product, or to accompany an article sold,¹⁵⁹ to add luster to the name of a corporation,¹⁶⁰ or for other business purposes.¹⁶¹ The statute in New York,¹⁶² and the others patterned after it¹⁶³ are limited by their terms to use for advertising or for "purposes of trade," and for that reason must be somewhat more narrow in their scope than the common law of the other states;¹⁶⁴ but in general, there has been no significant difference in their application in the field that they cover.

It is the plaintiff's name as a symbol of his identity that is involved here, and not his name as a mere name. There is, as a good many thousand John Smiths can bear witness, no such thing as an exclusive right to the use of any name. Unless there is some tortious use made of it, any one can be given or assume any name he likes.¹⁶⁵ The Kabotznicks may call themselves Cabots, and the Lovelskis become the Lowells, and the ancient proper Bostonian houses can do nothing about it but grieve. Any one may call himself Dwight D. Eisenhower, Henry Ford, Nelson Rockefeller, Eleanor Roosevelt, or Willie Mays, without any liability whatever. It is when he makes use of the name to pirate the plaintiff's identity for some advantage of his own, as by impersonation to obtain credit or secret information,¹⁶⁶ or by posing as the plaintiff's wife,¹⁶⁷ or providing a father for a child on a birth certificate,¹⁶⁸ that he becomes liable. It is in this sense that "appropriation" must be understood.

On this basis, the question before the courts has been first of all whether there has been appropriation of an aspect of the plaintiff's identity. It is not enough that a name which is the same as his is used in a novel,¹⁶⁹ a comic strip,¹⁷⁰ or the title of a corporation,¹⁷¹ unless

the context or the *circumstances*,¹⁷² or the addition of some other element,¹⁷³ indicate that the name is that of the plaintiff. It seems clear that a stage or other fictitious name can be so identified with the plaintiff that he is entitled to protection against its use.¹⁷⁴ On the other hand, there is no liability for the publication of a picture of his hand, leg and foot,¹⁷⁵ his dwelling house,¹⁷⁶ his automobile,¹⁷⁷ or his dog,¹⁷⁸ with nothing to indicate whose they are. Nor is there any liability when the plaintiff's character, occupation, and the general outline of his career, with many real incidents in his life, are used as the basis for a figure in a novel who is still clearly a fictional one.¹⁷⁹

Once the plaintiff is identified, there is the further question whether the defendant has appropriated the name or likeness for his own advantage. Under the statutes this must be a pecuniary advantage; but the common law is very probably not so limited.¹⁸⁰ The New York courts were faced very early with the obvious fact that newspapers and magazines, to say nothing of radio, television and motion pictures, are by no means philanthropic institutions, but are operated for profit. As against the contention that everything published by these agencies must necessarily be "for purposes of trade," they were compelled to hold that there must be some closer and more direct connection, beyond the mere fact that the newspaper is sold; and that the presence of advertising matter in adjacent columns does not make any difference.¹⁸¹ Any other conclusion would undoubtedly have been an unconstitutional interference with the freedom of the press.¹⁸² Accordingly, it has been held that the mere incidental mention of the plaintiff's name in a book¹⁸³ or a motion picture¹⁸⁴ or even in a commentary upon news which is part of an *advertisement*,¹⁸⁵ is not an invasion of his privacy; nor is the publication of a photograph¹⁸⁶ or a *newsreel*¹⁸⁷ in which he incidentally appears.

This liberality toward the publishers was brought to an abrupt termination, however, when cases began to appear in which false statements were made. It was held quite early in New York¹⁸⁸ that the publication of fiction concerning a man is a use of his name for purposes of trade, and that in such a case the mere sale of the article is enough in itself to provide the commercial element. It follows that when the name or the likeness is accompanied by false statements about the plaintiff,¹⁸⁹ or he is placed in a false light before the public,¹⁹⁰ there is such a use. The result of this rule for the encouragement of accuracy in the press is that the New York court has in fact recognized and applied the third form of invasion of privacy¹⁹¹ under a statute which was directed only at the fourth.

It seems sufficiently evident that appropriation is quite a different matter from intrusion, disclosure of private facts, or a false light in

the public eye. The interest protected is not so much a mental as a proprietary one, in the exclusive use of the plaintiff's name and likeness as an aspect of his identity. It seems quite pointless to dispute over whether such a right is to be classified as "property."¹⁹² If it is not, it is at least, once it is protected by the law, a right of value upon which the plaintiff can capitalize by selling licenses. Its proprietary nature is clearly indicated by a decision of the Second Circuit¹⁹³ that an exclusive license has what has been called a "right of publicity,"¹⁹⁴ which entitles him to enjoin the use of the name or likeness by a third person. Although this decision has not yet been followed,¹⁹⁵ it would seem clearly to be justified.

V. Common features

Judge Biggs has described the present state of the law of privacy as "still that of a haystack in a hurricane."¹⁹⁶ Disarray there certainly is; but almost all of the confusion is due to a failure to separate and distinguish these four forms of invasion, and to realize that they call for different things. Typical is the bewilderment which a good many members of the bar have expressed over the holdings in the two *Gill* cases in California. Both of them involved publicity given to the same photograph, taken while the plaintiff was embracing his wife in the Farmers' Market in Los Angeles. In one of them,¹⁹⁷ which involved only the question of disclosure by publishing the picture, it was held that there was nothing private about it, since it was a part of the public scene in a public place. In the other,¹⁹⁸ which involved the use of the picture to illustrate an article on the right and the wrong kind of love, with the innuendo that this was the wrong kind, liability was found for placing the plaintiff in a false light in the public eye. The two conclusions were based entirely upon the difference between the two branches of the tort.

Taking them in order—intrusion, disclosure, false light, and appropriation—the first and second require the invasion of something secret, secluded or private pertaining to the plaintiff; the third and fourth do not. The second and third depend upon publicity, while the first does not, nor does the fourth, although it usually involves it. The third requires falsity or fiction; the other three do not. The fourth involves a use for the defendant's advantage, which is not true of the rest. Obviously this is an area in which one must treat warily and be on the lookout for bogs. Nor is the difficulty decreased by the fact that quite often two or more of these forms of invasion may be found in the same case, and quite conceivably all four.¹⁹⁹

There has nevertheless been a good deal of consistency in the rules

that have been applied to the four disparate torts under the common name. As to any one of the four, it is agreed that the plaintiff's right is a personal one, which does not extend to the members of his family,²⁰⁰ unless, as is obviously possible,²⁰¹ their own privacy is invaded along with his. The right is not assignable,²⁰² and while the cause of action may²⁰³ or may not²⁰⁴ survive after his death, according to the survival rules of the particular state, there is no common law right of action for a publication concerning one who is already dead.²⁰⁵ The statutes of Oklahoma, Utah and Virginia,²⁰⁶ however, expressly provide for such an action. It seems to be generally agreed that the right of privacy is one pertaining only to individuals, and that a corporation²⁰⁷ or a partnership²⁰⁸ cannot claim it as such, although either may have an exclusive right to the use of its name, which may be protected upon some other basis such as that of unfair competition.²⁰⁹

So far as damages are concerned, there is general agreement that the plaintiff need not plead or prove special damages,²¹⁰ and that in this respect the action resembles one for libel or slander per se. The difficulty of measuring the damages is no more reason for denying relief here than in a defamation action.²¹¹ Substantial damages may be awarded for the presumed mental distress inflicted, and other probable harm, without proof.²¹² If there is evidence of special damage, such as resulting illness, or unjust enrichment of the defendant,²¹³ or harm to the plaintiff's own commercial interests,²¹⁴ it can be recovered. Punitive damages can be awarded upon the same basis as in other torts, where a wrongful motive or state of mind appears,²¹⁵ but not in cases where the defendant has acted innocently, as for example in the belief that the plaintiff has given his consent.²¹⁶

At an early stage of its existence, the right of privacy came into head-on collision with the constitutional guaranty of freedom of the press. The result was the slow evolution of a compromise between the two. Much of the litigation over privacy has been concerned with this compromise, which has involved two closely related, special and limited privileges arising out of the rights of the press.²¹⁷ One of these is the privilege of giving further publicity to already public figures. The other is that of giving publicity to news, and other matters of public interest. The one primarily concerns the person to whom publicity is given; the other the event, fact or other subject-matter. They are, however, obviously only different phases of the same thing.

VI. Public figures and public interest

A public figure has been defined as a person who, by his accomplishments, fame, or mode of living, or by adopting a profession or calling

which gives the public a legitimate interest in his doings, his affairs, and his character, has become a "public personage."²¹⁸ He is, in other words, a celebrity—one who by his own voluntary efforts has succeeded in placing himself in the public eye. Obviously to be included in this category are those who have achieved at least some degree of reputation²¹⁹ by appearing before the public, as in the case of an actor,²²⁰ a professional baseball player,²²¹ a pugilist,²²² or any other entertainer.²²³ The list is, however, broader than this. It includes public officers,²²⁴ famous inventors²²⁵ and explorers,²²⁶ war heroes²²⁷ and even ordinary soldiers,²²⁸ an infant prodigy,²²⁹ and no less a personage than the Grand Exalted Ruler of a lodge.²³⁰ It includes, in short, any one who has arrived at a position where public attention is focused upon him as a person. It seems clear, however, that such public stature must already exist before there can be any privilege arising out of it, and that the defendant, by directing attention to one who is obscure and unknown, cannot himself create a public figure.²³¹

Such public figures are held to have lost, to some extent at least, their right of privacy. Three reasons are given, more or less indiscriminately, in the decisions: that they have sought publicity and consented to it, and so cannot complain of it; that their personalities and their affairs already have become public, and can no longer be regarded as their own private business; and that the press has a privilege, guaranteed by the Constitution, to inform the public about those who have become legitimate matters of public interest. On one or another of these grounds, and sometimes all, it is held that there is no liability when they are given additional publicity, as to matters reasonably within the scope of the public interest which they have aroused.²³²

The privilege of giving publicity to news, and other matters of public interest, arises out of the desire and the right of the public to know what is going on in the world, and the freedom of the press and other agencies of information to tell them. "News" includes all events and items of information which are out of the ordinary humdrum routine, and which have "that indefinable quality of information which arouses public attention."²³³ To a very great extent the press, with its experience or instinct as to what its readers will want, has succeeded in making its own definition of news. A glance at any morning newspaper will sufficiently indicate the content of the term. It includes homicide²³⁴ and other crimes,²³⁵ arrests²³⁶ and police raids,²³⁷ suicides,²³⁸ marriages²³⁹ and divorces,²⁴⁰ accidents,²⁴¹ a death from the use of narcotics,²⁴² a woman with a rare disease,²⁴³ the birth of a child to a twelve year old girl,²⁴⁴ the filing of a libel suit,²⁴⁵ a report to the police concerning the escape of a black panther,²⁴⁶ the reappearance of one supposed to have been murdered years ago,²⁴⁷ and undoubtedly many other sim-

ilar matters of genuine, if more or less deplorable, popular appeal.²⁴⁸

The privilege of enlightening the public is not, however, limited to the dissemination of news in the sense of current events. It extends also to information or education, or even entertainment and amusement,²⁴⁹ by books, articles, pictures, films and broadcasts concerning interesting phases of human activity in general,²⁵⁰ and the reproduction of the public scene as in newsreels and travelogues.²⁵¹ In determining where to draw the line the courts have been invited to exercise nothing less than a power of censorship over what the public may be permitted to read; and they have been understandably liberal in allowing the benefit of the doubt.

Caught up and entangled in this web of news and public interest are a great many people who have not sought publicity, but indeed, as in the case of the accused criminal, have tried assiduously to avoid it. They have nevertheless lost some part of their right of privacy. The misfortunes of the frantic woman whose husband is murdered before her eyes,²⁵² or the innocent bystander who is caught in a raid on a cigar store and mistaken by the police for the proprietor,²⁵³ can be broadcast to the world, and they have no remedy. Such individuals become public figures²⁵⁴ for a season; and "until they have reverted to the lawful and unexciting life led by the great bulk of the community, they are subject to the privileges which publishers have to satisfy the curiosity of the public as to their leaders, heroes, villains and victims."²⁵⁵ The privilege extends even to identification and some reasonable depiction of the individual's family,²⁵⁶ although there must certainly be limits as to their own private lives into which the publisher cannot go.²⁵⁷

What is called for, in short, is some logical connection between the plaintiff and the matter of public interest. The most extreme cases of the privilege are those in which the likeness of an individual is used to illustrate a book or an article on some general topic, rather than any specific event. Where this is appropriate and pertinent, as where the picture of a strikebreaker is used to illustrate a book on strike-breaking,²⁵⁸ or that of a Hindu illusionist is employed to illustrate an article on the Indian rope trick,²⁵⁹ it has been held that there is no liability, since the public interest justifies any invasion of privacy. On the other hand, where the illustration is not pertinent, and a connection is suggested which does not exist, as where the face of an honest taxi driver appears in connection with an article on the cheating practices of the trade,²⁶⁰ or the picture of a decent model illustrates one on "man hungry" women,²⁶¹ the plaintiff is placed in a false light, and may recover on that basis. The difference is well brought out by two cases in California and New York. In one of them²⁶² a photograph

of the plaintiff arguing with a would-be suicide on a bridge was held properly used to illustrate an article on suicide. In the other²⁶³ the picture of a boy in the slums, taken while he was innocently talking baseball on the street, was used with an article about juvenile delinquency, entitled "Gang Boy," and he was allowed to recover.

VII. Limitations

It is clear, however, that the public figure loses his right of privacy only to a limited extent,²⁶⁴ and that the privilege of reporting news and matters of public interest is likewise limited. The decisions indicate very definitely that both privileges apply only to one branch of the tort, that of disclosure of private facts about the individual. The famous motion picture actress who "wants to be alone"²⁶⁵ unquestionably has as much right as any one else to be free from intrusion into her home or her bank account; and so has the individual whose divorce is the sensation of the day.²⁶⁶ The celebrity can undoubtedly complain of the appropriation of his name or likeness for purposes of advertising, or the sale of a product,²⁶⁷ and so can the victim of an accident.²⁶⁸ It was once held that even the Emperor of Austria had a right to object when his name was bestowed on an insurance company.²⁶⁹ And while it seems to be agreed that the courts are not arbiters of taste, and the fact that a publication is morbid, gruesome, lurid, sensational, immoral, and altogether cheap and despicable will not forfeit the privilege,²⁷⁰ it is also clear that either the public figure²⁷¹ or the man in the news²⁷² can maintain an action when false or fictitious statements are published about him, or when his picture is used with an innuendo which places him in a false light before the public.²⁷³

But even as to the disclosure of private facts, it appears that there must be some rather undefined limits upon these privileges. Warren and Brandeis²⁷⁴ thought that even a celebrity was entitled to his private life, and that he would become a public figure only as to matters already public and those which directly bore upon them. The development of the law has not been so narrow. It has recognized a legitimate public curiosity about the personalities of celebrities, and about a great deal of otherwise private and personal information concerning them. Their biographies can be written,²⁷⁵ and their life histories and their characters set forth before the world in unflattering detail. Discreditable facts about them can be exposed.²⁷⁶ And as our newspapers demonstrate daily, the public can be treated to an enormous amount of petty gossip as to what they eat for breakfast, wear, read, do with their spare time, or say to their friends.

Some boundaries, however, still remain; and one may venture the

guess that the private sex relations of actresses and baseball players, to say nothing of inventors and the victims of automobile accidents, are still not in the public domain.²⁷⁷ As some evidence of popular feeling in such matters, one might look to the statutes in several states²⁷⁸ prohibiting the public disclosure of the names of victims of sex crimes. The private letters, even of celebrities, cannot be published without their consent;²⁷⁹ and the good Prince Albert was once held to have an action when his private etchings were exhibited to all comers.²⁸⁰ An excellent illustration of the privacy of a public figure is a case²⁸¹ in a trial court in Los Angeles, not officially reported, in which the actor Kirk Douglas, after engaging in some undignified antics before a home motion picture camera for his friends, was held to have a cause of action when the film was put upon public exhibition.

Very probably there is some rough proportion to be looked for, between the importance of the public figure or the man in the news, and of the occasion for the public interest in him, and the nature of the private facts revealed. Perhaps there is very little in the way of information about the President of the United States, or any candidate for that high office,²⁸² that is not a matter of legitimate public concern; but when a mere member of the armed forces is in question, the line is drawn at his military service, and those things that more or less directly bear upon it.²⁸³ And no doubt the defendant in a spectacular murder trial which draws national attention can expect a good deal less in the way of privacy than an ordinary citizen who is arrested for ignoring a parking ticket. But thus far there is very little in the cases to indicate just where such lines are to be drawn.

One troublesome question, which cannot be said to have been fully resolved, is that of the effect of lapse of time, during which the plaintiff has returned to obscurity. There can be no doubt that one quite legitimate function of the press is that of educating or reminding the public as to past history, and that the recall of former public figures, the revival of past events that once were news, can properly be a matter of present public interest. If it is only the event itself which is recalled, without the use of the plaintiff's name, there seems to be no doubt that even a great lapse of time does not destroy the privilege.²⁸⁴ Most of the cases have held that even the use of his name²⁸⁵ or likeness²⁸⁶ is not enough in itself to lead to liability. Thus a luckless prosecuting attorney who once made the mistake of allowing himself to be photographed with his arm around a noted criminal was held to have no remedy when the picture was republished fifteen years later in connection with a story of the criminal's career.²⁸⁷ Such decisions indicate that once a man has become a public figure, or news, he remains a

matter of legitimate recall to the public mind to the end of his days.

There is, however, *Melvin v. Reid*,²⁸⁸ in which it was held that the use of the name of a former prostitute and murder defendant made the publisher liable when a motion picture narrated her story; and there are a few other cases²⁸⁹ that look in the same direction. One may speculate that the real reason for the decision in the *Melvin* case was not the use of the name in connection with past history, but the disclosure of the plaintiff's whereabouts and identity, which were no part of the revived "news," or perhaps that the explanation lay in the shocking enormity of the revelation of a woman's past when she was trying to lead a decent life, and that again something in the nature of a "mores" test is to be applied. There is, however, almost nothing in the cases to throw any satisfactory light upon such speculations. All that can be said is that there appear to be situations in which ancient history cannot safely be revived.

VIII. Defenses

Next in order are the various defenses to the claim of invasion of privacy. It is clear first of all that the truth of the matter published does not arise in the cases of intrusion, and can be no defense to the appropriation of name or likeness, nor to the public disclosure of private facts.²⁹⁰ It may, however, be in issue where the third form of the tort is involved, that of putting the plaintiff in a false light in the public eye,²⁹¹ and to that extent it has some limited importance, and cannot be entirely ruled out.

Chief among the available defenses is that of the plaintiff's consent to the invasion, which will bar his recovery as in the case of any other tort.²⁹² It may be given expressly, or by conduct, such as posing for a picture with knowledge of the purposes for which it is to be used,²⁹³ or industriously seeking publicity of the same kind.²⁹⁴ A gratuitous consent can be revoked at any time before the invasion;²⁹⁵ but if the agreement is a matter of contract it is normally irrevocable, and there is no liability for any publicity or appropriation within its terms.²⁹⁶ But if the actual invasion goes beyond the contract, fairly construed, as by alteration of the plaintiff's picture,²⁹⁷ or publicity materially differing in kind or in extent from that contemplated,²⁹⁸ the consent is not effective to avoid liability. The statutes²⁹⁹ all require that the consent be given in writing. As against the contention that this can still be "waived" by consent given orally, the rule which has emerged in New York is that the oral consent will not bar the cause of action, but is to be taken into account in mitigation of damages.³⁰⁰

Other defenses have appeared only infrequently. Warren and Brandeis³⁰¹ thought that the action for invasion of privacy must be subject to any privilege which would justify the publication of libel or slander, reasoning that that which is true should be no less privileged than that which is false. There is still no reason to doubt this conclusion, since the absolute privilege of a witness,³⁰² and the qualified one to report the filing of a nominating petition for office³⁰³ or the pleadings in a civil suit³⁰⁴ have both been recognized. The privilege of the defendant to protect or further his own legitimate interests has appeared in a case or two, where a telephone company has been permitted to monitor calls,³⁰⁵ and the defendant was allowed to make use of the plaintiff's name in insuring his wife without his consent.³⁰⁶ It has been held that where ~~uncopyrighted~~ literature is in the public domain, and the defendant is free to publish it, the name of the plaintiff may be used to indicate its authorship,³⁰⁷ and that when the plaintiff has designed dresses for the defendant it is no invasion of his privacy to disclose his connection with the product in advertising.³⁰⁸

The conflict of laws, so far as the right of privacy is concerned, is in the same state of bewildered confusion as that which surrounds the law of defamation. The writer has attempted to deal with it elsewhere,³⁰⁹ and will not repeat it here.

Conclusion

It is evident from the foregoing that, by the use of a single word supplied by Warren and Brandeis, the courts have created an independent basis of liability, which is a complex of four distinct and only loosely related torts; and that this has been expanded by slow degrees to invade, overlap, and encroach upon a number of other fields. So far as appears from the decisions, the process has gone on without any plan, without much realization of what is happening or its significance, and without any consideration of its dangers. They are nonetheless sufficiently obvious, and not to be overlooked.

One cannot fail to be aware, in reading privacy cases, of the extent to which defenses, limitations and safeguards established for the protection of the defendant in other tort fields have been jettisoned, disregarded, or ignored. Taking intrusion first, the gist of the wrong is clearly the intentional infliction of mental distress, which is now in itself a recognized basis of tort liability.³¹⁰ Where such mental disturbance stands on its own feet, the courts have insisted upon extreme outrage, rejecting all liability for trivialities, and upon genuine and

serious mental harm, attested by physical illness, or by the circumstances of the case. But once "privacy" gets into the picture, and the fact of the intrusion is added, such guarantees apparently are no longer required. No doubt the cases thus far have been sufficiently extreme; but the question may well be raised whether there are not some limits, and whether, for example, a lady who insists upon sunbathing in the nude in her own back yard should really have a cause of action for her humiliation when the neighbors examine her with appreciation and binoculars.

The public disclosure of private facts, and putting the plaintiff in a false light in the public eye, both concern the interest in reputation, and move into the field occupied by defamation. Here, as a result of some centuries of conflict, there have been jealous safeguards thrown about the freedom of speech and of the press, which are now turned on the left flank. Gone is the defense of truth, and the defendant is held liable for the publication of entirely accurate statements of fact, without any wrongful motive. Gone also is the requirement of special damage, where what is said is not libel or slander "per se"—which, however antiquated and unreasonable the rigid categories may be, has at least served some useful purpose in the discouragement of trivial and extortionate claims. Gone even is the need for any defamatory innuendo at all, since the publication of nondefamatory facts, or of even laudatory fiction concerning the plaintiff, may be enough. The retraction statutes, with their provision for demand upon the defendant, and the limitation to proved special damage if a demand is not made or is complied with, are circumvented; and so are the statutes requiring the filing of a bond for costs before a defamation action can be begun. These are major inroads upon a right to which there has always been much sentimental devotion in our land; and they have gone almost entirely ~~unremarked~~. Perhaps more important still is the extent to which, under any test of "ordinary sensibilities," or the "mores" of the community as to what is acceptable and proper, the courts, although cautiously and reluctantly, have accepted a power of censorship over what the public may be permitted to read, extending very much beyond that which they have always had under the law of defamation.

As for the appropriation cases, they create in effect, for every individual, a common law trade name, his own, and a common law trade mark in his likeness. They confer upon him rights much more extensive than those which any corporation engaged in business can expect under the law of unfair competition. These rights are subject to the verdict of a jury. And there has been no hint that they are in

any way affected by any of the limitations which have been considered necessary and desirable in the ordinary law of trade marks and trade names.

This is not to say that the developments in the law of privacy are wrong. Undoubtedly they have been supported by genuine public demand and lively public feeling, and made necessary by real abuses on the part of defendants who have brought it all upon themselves. It is to say rather that it is high time that we realize what we are doing, and give some consideration to the question of where, if anywhere, we are to call a halt.

All this is a most marvelous tree to grow from the wedding of the daughter of Mr. Samuel D. Warren. One is tempted to surmise that she must have been a very beautiful girl. Resembling, perhaps, that fabulous creature, the daughter of a Mr. Very, a confectioner in Regent Street, who was so wondrous fair that her presence in the shop caused three or four hundred people to assemble every day in the street before the window to look at her, so that her father was forced to send her out of town, and counsel was led to inquire whether she might not be indicted as a public nuisance.³¹¹ This was the face that launched a thousand lawsuits.

NOTES

1 "The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle. The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury." Warren and Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 196 (1890).

2 Mason, Brandeis, *A Free Man's Life* 70 (1946).

3 4 Harv. L. Rev. 193 (1890).

4 Woolsey v. Judd, 4 Duer (11 N.Y. Super.) 379, 11 How. Pr. 49 (N.Y. 1855) (publication of private letters); Gee v. Pritchard, 2 Swans. 402, 36 Eng. Rep. 670 (1818) (same); Prince Albert v. Strange, 2 De G. & Sm. 652, 41

Eng. Rep. 1171, 1 Mac. & G. 25, 64 Eng. Rep. 293 (1849) (exhibition of etchings and publication of catalogue).

- 5 Yovatt v. Winyard, 1 Jac. & W. 394, 37 Eng. Rep. 425 (1820) (publication of recipes surreptitiously obtained by employee); Abernethy v. Hutchinson, 3 L.J. Ch. 109 (1825) (publication of lectures to class of which defendant was a member); Pollard v. Photographic Co., 40 Ch. D. 345 (1888) (publication of plaintiff's picture made by defendant).
- 6 Larremore, *The Law of Privacy*, 12 Colum. L. Rev. 693 (1912); Ragland, *The Right of Privacy*, 17 Ky. L.J. 101 (1929); Winfield, *Privacy*, 47 L.Q. Rev. 23 (1931); Green, *The Right of Privacy*, 27 Ill. L. Rev. 237 (1932); Kacedan, *The Right of Privacy*, 12 B.U.L. Rev. 353, 600 (1932); Dickler, *The Right of Privacy*, 70 U.S.L. Rev. 435 (1936); Harper & McNeely, *A Re-examination of the Basis for Liability for Emotional Distress*, [1938] Wis. L. Rev. 426; Nizer, *The Right of Privacy*, 39 Mich. L. Rev. 526 (1941); Feinberg, *Recent Developments in the Law of Privacy*, 48 Colum. L. Rev. 713 (1948); Ludwig, "Peace of Mind" in *48 Pieces vs. Uniform Right of Privacy*, 32 Minn. L. Rev. 734 (1948); Yankwich, *The Right of Privacy*, 27 Notre Dame Law. 429 (1952); Daims, *What Do We Mean by "Right to Privacy"*, 4 S.D.L. Rev. 1 (1959).

Also Notes in 8 Mich. L. Rev. 221 (1909); 12 Colum. L. Rev. 1 (1912); 43 Harv. L. Rev. 297 (1929); 7 N.C.L. Rev. 435 (1929); 26 Ill. L. Rev. 63 (1931); 81 U. Pa. L. Rev. 324 (1933); 33 Ill. L. Rev. 87 (1938); 13 So. Cal. L. Rev. 81 (1939); 15 Temp. L.Q. 148 (1941); 25 Minn. L. Rev. 619 (1941); 30 Cornell L.Q. 398 (1945); 48 Colum. L. Rev. 713 (1948); 15 U. Chi. L. Rev. 926 (1948); 6 Ark. L. Rev. 459 (1952); 38 Va. L. Rev. 117 (1952); 28 Ind. L.J. 179 (1953); 27 Miss. L.J. 256 (1956); 44 Va. L. Rev. 1303 (1958); 31 Miss. L.J. 191 (1960).

The foreign law is discussed in Gutteridge, *The Comparative Law of the Right to Privacy*, 47 L.Q. Rev. 203 (1931); Walton, *The Comparative Law of the Right to Privacy*, 47 L.Q. Rev. 219 (1960).

- 7 O'Brien, *The Right of Privacy*, 2 Colum. L. Rev. 437 (1902); Lisle, *The Right of Privacy (A Contra View)*, 19 Ky. L.J. 137 (1931); Notes, 2 Colum. L. Rev. 437 (1902); 64 Albany L.J. 428 (1902); 29 Law Notes 64 (1925); 43 Harv. L. Rev. 297 (1929); 26 Ill. L. Rev. 63 (1931).

- 8 Manela v. Stevens (N.Y. Sup. Ct. 1890), in N.Y. Times, June 15, 18, 21, 1890.

- 9 Mackenzie v. Soden Mineral Springs Co., 27 Abb. N. Cas. 402, 18 N.Y.S. 240 (Sup. Ct. 1891) (use of name of physician in advertising patent medicine enjoined); Marks v. Jaffa, 6 Misc. 290, 26 N.Y.S. 908 (Super. Ct. N.Y. City 1893) (entering actor in embarrassing popularity contest); Schuyler v. Curtis, 147 N.Y. 434, 42 N.E. 22 (1895) (erection of statue as memorial to deceased; relief denied only because he was dead).

- 10 Corliss v. E. W. Walker Co., 64 Fed. 280 (D. Mass. 1894) (portrait to be inserted in biographical sketch of plaintiff; relief denied because he was a public figure).

- 11 Atkinson v. John E. Doherty & Co., 121 Mich. 372, 80 N.W. 285 (1899).

JAMES RACHELS

Why Privacy Is Important

According to Thomas Scanlon, the first element of a theory of privacy should be “a characterization of the special interest we have in being able to be free from certain kinds of intrusions.” Since I agree that is the right place to begin, I shall begin there. Then I shall comment briefly on Judith Jarvis Thomson’s proposals.

I

Why, exactly, is privacy important to us? There is no one simple answer to this question, since people have a number of interests that may be harmed by invasions of their privacy.

(a) Privacy is sometimes necessary to protect people’s interests in competitive situations. For example, it obviously would be a disadvantage to Bobby Fischer if he could not analyze the adjourned position in a chess game in private, without his opponent learning his results.

(b) In other cases someone may want to keep some aspect of his life or behavior private simply because it would be embarrassing for other people to know about it. There is a splendid example of this in John Barth’s novel *End of the Road*. The narrator of the story, Jake Horner, is with Joe Morgan’s wife, Rennie, and they are approaching the Morgan house where Joe is at home alone:

“Want to eavesdrop?” I whispered impulsively to Rennie. “Come on, it’s great! See the animals in their natural habitat.”

Rennie looked shocked. “What for?”

"You mean you never spy on people when they're alone? It's wonderful! Come on, be a sneak! It's the most unfair thing you can do to a person."

"You disgust me, Jake!" Rennie hissed. "He's just reading. You don't know Joe at all, do you?"

"What does that mean?"

"Real people aren't any different when they're alone. No masks. What you see of them is authentic."

. . . Quite reluctantly, she came over to the window and peeped in beside me.

It is indeed the grossest of injustices to observe a person who believes himself to be alone. Joe Morgan, back from his Boy Scout meeting, had evidently intended to do some reading, for there were books lying open on the writing table and on the floor beside the bookcase. But Joe wasn't reading. He was standing in the exact center of the bare room, fully dressed, smartly executing military commands. About *face!* Right *dress!* 'Ten-shun! Parade *rest!* He saluted briskly, his cheeks blown out and his tongue extended, and then proceeded to cavort about the room—spinning, pirouetting, bowing, leaping, kicking. I watched entranced by his performance, for I cannot say that in my strangest moments (and a bachelor has strange ones) I have surpassed him. Rennie trembled from head to foot.¹

The scene continues even more embarrassingly.

(c) There are several reasons why medical records should be kept private, having to do with the consequences to individuals of facts about them becoming public knowledge. "The average patient doesn't realize the importance of the confidentiality of medical records. Passing out information on venereal disease can wreck a marriage. Revealing a pattern of alcoholism or drug abuse can result in a man's losing his job or make it impossible for him to obtain insurance protection."²

(d) When people apply for credit (or for large amounts of insurance or for jobs of certain types) they are often investigated, and the

1. John Barth, *End of the Road* (New York, 1960), pp. 57-58.

2. Dr. Malcolm Todd, President of the A.M.A., quoted in the *Miami Herald*, 26 October 1973, p. 18-A.

result is a fat file of information about them. Now there is something to be said in favor of such investigations, for business people surely do have the right to know whether credit-applicants are financially reliable. The trouble is that all sorts of other information goes into such files, for example, information about the applicant's sex-life, his political views, and so forth. Clearly it is unfair for one's application for credit to be influenced by such irrelevant matters.

These examples illustrate the variety of interests that may be protected by guaranteeing people's privacy, and it would be easy to give further examples of the same general sort. However, I do not think that examining such cases will provide a complete understanding of the importance of privacy, for two reasons.

First, these cases all involve relatively unusual sorts of situations, in which someone has something to hide or in which information about a person might provide someone with a reason for mistreating him in some way. Thus, reflection on these cases gives us little help in understanding the value which privacy has in *normal* or *ordinary* situations. By this I mean situations in which there is nothing embarrassing or shameful or unpopular in what we are doing, and nothing ominous or threatening connected with its possible disclosure. For example, even married couples whose sex-lives are normal (whatever that is), and so who have nothing to be ashamed of, by even the most conventional standards, and certainly nothing to be blackmailed about, do not want their bedrooms bugged. We need an account of the value which privacy has for us, not only in the few special cases but in the many common and unremarkable cases as well.

Second, even those invasions of privacy that *do* result in embarrassment or in some specific harm to our other interests are objectionable on other grounds. A woman may rightly be upset if her credit-rating is adversely affected by a report about her sexual behavior because the use of such information is unfair; however, she may also object to the report simply because she feels—as most of us do—that her sex-life is *nobody else's business*. This, I think, is an extremely important point. We have a “sense of privacy” which is violated in such affairs, and this sense of privacy cannot adequately be explained merely in terms of our fear of being embarrassed or disadvantaged in one of these obvious ways. An adequate account of privacy should

help us to understand what makes something "someone's business" and why intrusions into things that are "none of your business" are, as such, offensive.

These considerations lead me to suspect that there is something important about privacy which we shall miss if we confine our attention to examples such as (a), (b), (c), and (d). In what follows I will try to bring out what this something is.

II

I want now to give an account of the value of privacy based on the idea that there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people. According to this account, privacy is necessary if we are to maintain the variety of social relationships with other people that we want to have, and that is why it is important to us. By a "social relationship" I do not mean anything especially unusual or technical; I mean the sort of thing which we usually have in mind when we say of two people that they are friends or that they are husband and wife or that one is the other's employer.

The first point I want to make about these relationships is that, often, there are fairly definite patterns of behavior associated with them. Our relationships with other people determine, in large part, how we act toward them and how they behave toward us. Moreover, there are *different* patterns of behavior associated with different relationships. Thus a man may be playful and affectionate with his children (although sometimes firm), businesslike with his employees, and respectful and polite with his mother-in-law. And to his close friends he may show a side of his personality that others never see—perhaps he is secretly a poet, and rather shy about it, and shows his verse only to his best friends.

It is sometimes suggested that there is something deceitful or hypocritical about such differences in behavior. It is suggested that underneath all the role-playing there is the "real" person, and that the various "masks" that we wear in dealing with some people are some sort of phony disguise that we use to conceal our "true" selves from them. I take it that this is what is behind Rennie's remark, in

the passage from Barth, that, "Real people aren't any different when they're alone. No masks. What you see of them is authentic." According to this way of looking at things, the fact that we observe different standards of conduct with different people is merely a sign of dishonesty. Thus the cold-hearted businessman who reads poetry to his friends is "really" a gentle poetic soul whose businesslike demeanor in front of his employees is only a false front; and the man who curses and swears when talking to his friends, but who would never use such language around his mother-in-law, is just putting on an act for her.

This, I think, is quite wrong. Of course the man who does not swear in front of his mother-in-law may be just putting on an act so that, for example, she will not disinherit him, when otherwise he would curse freely in front of her without caring what she thinks. But it may be that his conception of how he ought to behave with his mother-in-law is very different from his conception of how he may behave with his friends. Or it may not be appropriate for him to swear around *her* because "she is not that sort of person." Similarly, the businessman may be putting up a false front for his employees, perhaps because he dislikes his work and has to make a continual, disagreeable effort to maintain the role. But on the other hand he may be, quite comfortably and naturally, a businessman with a certain conception of how it is appropriate for a businessman to behave; and this conception is compatible with his also being a husband, a father, and a friend, with different conceptions of how it is appropriate to behave with his wife, his children, and his friends. There need be nothing dishonest or hypocritical in any of this, and neither side of his personality need be the "real" him, any more than any of the others.

It is not merely accidental that we vary our behavior with different people according to the different social relationships that we have with them. Rather, the different patterns of behavior are (partly) what define the different relationships; they are an important part of what makes the different relationships what they are. The relation of friendship, for example, involves bonds of affection and special obligations, such as the duty of loyalty, which friends owe to one another; but it is also an important part of what it means to have a

friend that we welcome his company, that we confide in him, that we tell him things about ourselves, and that we show him sides of our personalities which we would not tell or show to just anyone.³ Suppose I believe that someone is my close friend, and then I discover that he is worried about his job and is afraid of being fired. But, while he has discussed this situation with several other people, he has not mentioned it at all to me. And then I learn that he writes poetry, and that this is an important part of his life; but while he has shown his poems to many other people, he has not shown them to me. Moreover, I learn that he behaves with his other friends in a much more informal way than he behaves with me, that he makes a point of seeing them socially much more than he sees me, and so on. In the absence of some special explanation of his behavior, I would have to conclude that we are not as close as I had thought.

The same general point can be made about other sorts of human relationships: businessman to employee, minister to congregant, doctor to patient, husband to wife, parent to child, and so on. In each case, the sort of relationship that people have to one another involves a conception of how it is appropriate for them to behave with each other, and what is more, a conception of the kind and degree of knowledge concerning one another which it is appropriate for them to have. (I will say more about this later.) I do not mean to imply that such relationships are, or ought to be, structured in exactly the same way for everyone. Some parents are casual and easy-going with their children, while others are more formal and reserved. Some doctors want to be friends with at least some of their patients; others are businesslike with all. Moreover, the requirements of social roles may vary from community to community—for example, the role of wife may not require exactly the same sort of behavior in rural Alabama as it does in New York or New Guinea. And, the requirements of social roles may change: the women's liberation movement is making an attempt to redefine the husband-wife relationship. The examples that I have been giving are drawn, loosely speaking, from contemporary American society; but this is mainly a matter of convenience. The only point that I want to insist on is that *however* one

3. My view about friendship and its relation to privacy is similar to Charles Fried's view in his book *An Anatomy of Values* (Cambridge, Mass., 1970).

conceives one's relations with other people, there is inseparable from that conception an idea of how it is appropriate to behave with and around them, and what information about oneself it is appropriate for them to have.

The point may be underscored by observing that new types of social institutions and practices sometimes make possible new sorts of human relationships, which in turn make it appropriate to behave around people, and to say things in their presence, that would have been inappropriate before. "Group therapy" is a case in point. Many psychological patients find the prospect of group therapy unsettling, because they will have to speak openly to the group about intimate matters. They sense that there is something inappropriate about this: one simply does not reveal one's deepest feelings to strangers. Our aspirations, our problems, our frustrations and disappointments are things that we may confide to our husbands and wives, our friends, and perhaps to some others—but it is out of the question to speak of such matters to people that we do not even know. Resistance to this aspect of group therapy is overcome when the patients begin to think of each other not as strangers but as *fellow members of the group*. The definition of a kind of relation between them makes possible frank and intimate conversation which would have been totally out of place when they were merely strangers.

All of this has to do with the way that a crucial part of our lives—our relations with other people—is organized, and as such its importance to us can hardly be exaggerated. Thus we have good reason to object to anything that interferes with these relationships and makes it difficult or impossible for us to maintain them in the way that we want to. Conversely, because our ability to control who has access to us, and who knows what about us, allows us to maintain the variety of relationships with other people that we want to have, it is, I think, one of the most important reasons why we value privacy.

First, consider what happens when two close friends are joined by a casual acquaintance. The character of the group changes; and one of the changes is that conversation about intimate matters is now out of order. Then suppose these friends could *never* be alone; suppose there were always third parties (let us say casual acquaintances or strangers) intruding. Then they could do either of two things. They

could carry on as close friends do, sharing confidences, freely expressing their feelings about things, and so on. But this would mean violating their sense of how it is appropriate to behave around casual acquaintances or strangers. Or they could avoid doing or saying anything which they think inappropriate to do or say around a third party. But this would mean that they could no longer behave with one another in the way that friends do and further that, eventually, they would no longer *be* close friends.

Again, consider the differences between the way that a husband and wife behave when they are alone and the way they behave in the company of third parties. Alone, they may be affectionate, sexually intimate, have their fights and quarrels, and so on; but with others, a more "public" face is in order. If they could never be alone together, they would either have to abandon the relationship that they would otherwise have as husband and wife or else behave in front of others in ways they now deem inappropriate.⁴

These considerations suggest that we need to separate our associations, at least to some extent, if we are to maintain a system of different relationships with different people. Separation allows us to behave with certain people in the way that is appropriate to the sort of relationship we have with them, without at the same time violating our

4. I found this in a television program-guide in the *Miami Herald*, 21 October 1973, p. 17:

"I think it was one of the most awkward scenes I've ever done," said actress Brenda Benet after doing a romantic scene with her husband, Bill Bixby, in his new NBC-TV series, "The Magician."

"It was even hard to kiss him," she continued. "It's the same old mouth, but it was terrible. I was so abnormally shy; I guess because I don't think it's anybody's business. The scene would have been easier had I done it with a total stranger because that would be real acting. With Bill, it was like being on exhibition."

I should stress that, on the view that I am defending, it is *not* "abnormal shyness" or shyness of any type that is behind such feelings. Rather, it is a sense of what is appropriate with and around people with whom one has various sorts of personal relationships. Kissing *another actor* in front of the camera crew, the director, and so on, is one thing; but kissing *one's husband* in front of all these people is quite another thing. What made Ms. Benet's position confusing was that her husband *was* another actor, and the behavior that was permitted by the one relationship was discouraged by the other.

sense of how it is appropriate to behave with, and in the presence of, others with whom we have a different kind of relationship. Thus, if we are to be able to control the relationships that we have with other people, we must have control over who has access to us.

We now have an explanation of the value of privacy in ordinary situations in which we have nothing to hide. The explanation is that, even in the most common and unremarkable circumstances, we regulate our behavior according to the kinds of relationships we have with the people around us. If we cannot control who has access to us, sometimes including and sometimes excluding various people, then we cannot control the patterns of behavior we need to adopt (this is one reason why privacy is an aspect of liberty) or the kinds of relations with other people that we will have. But what about our feeling that certain facts about us are "simply nobody else's business"? Here, too, I think the answer requires reference to our relationships with people. If someone is our doctor, then it literally is his business to keep track of our health; if someone is our employer, then it literally is his business to know what salary we are paid; our financial dealings literally are the business of the people who extend us credit; and so on. In general, a fact about ourselves is someone's business if there is a specific social relationship between us which entitles them to know. We are often free to choose whether or not to enter into such relationships, and those who want to maintain as much privacy as possible will enter them only reluctantly. What we cannot do is accept such a social role with respect to another person and then expect to retain the same degree of privacy relative to him that we had before. Thus, if we are asked how much money we have in the bank, we cannot say, "It's none of your business," to our banker, to prospective creditors, or to our spouses, because their relationships with us do entitle them to know. But, at the risk of being boorish, we could say that to others with whom we have no such relationship.

III

Thomson suggests, "as a simplifying hypothesis, that the right to privacy is itself a cluster of rights, and that it is not a distinct cluster of rights but itself intersects with the cluster of rights which the

right over the person consists of, and also with the cluster of rights which owning property consists of." This hypothesis is "simplifying" because it eliminates the right to privacy as anything distinctive.

"The right over the person" consists of such "un-grand" rights as the right not to have various parts of one's body looked at, the right not to have one's elbow painted green, and so on. Thomson understands these rights as analogous to property rights. The idea is that our bodies are *ours* and so we have the same rights with respect to them that we have with respect to our other possessions.

But now consider the right not to have various parts of one's body looked at. Insofar as this is a matter of *privacy*, it is not simply analogous to property rights; for the kind of interest we have in controlling who looks at what parts of our bodies is very different from the interest we have in our cars or fountain pens. For most of us, physical intimacy is a part of very special sorts of personal relationships. Exposing one's knee or one's face to someone may not count for us as physical intimacy, but exposing a breast, and allowing it to be seen and touched, does. Of course the details are to some extent a matter of social convention; that is why it is easy for us to imagine, say, a Victorian woman for whom an exposed knee would be a sign of intimacy. She would be right to be distressed at learning that she had absent-mindedly left a knee uncovered and that someone was looking at it—if the observer was not her spouse or her lover. By dissociating the body from ideas of physical intimacy, and the complex of personal relationships of which such intimacies are a part, we can make this "right over the body" seem to be nothing more than an un-grand kind of property right; but that dissociation separates this right from the matters that make *privacy* important.

Thomson asks whether it violates your right to privacy for acquaintances to indulge in "very personal gossip" about you, when they got the information without violating your rights, and they are not violating any confidences in telling what they tell. (See part VIII, case (e), in Thomson's paper.) She thinks they do not violate your right to privacy, but that if they do "there is trouble for the simplifying hypothesis."

This is, as she says, a debatable case, but if my account of why privacy is important is correct, we have at least some reason to think

that your right to privacy can be violated in such a case. Let us fill in some details. Suppose you are recently divorced, and the reason your marriage failed is that you became impotent shortly after the wedding. You have shared your troubles with your closest friend, but this is not the sort of thing you want everyone to know. Not only would it be humiliating for everyone to know, it is none of their business. It is the sort of intimate fact about you that is not appropriate for strangers or casual acquaintances to know. But now the gossips have obtained the information (perhaps one of them innocently overheard your discussion with your friend; it was not his fault, so he did not violate your privacy in the hearing, but then you did not know he was within earshot) and now they are spreading it around to everyone who knows you and to some who do not. Are they violating your right to privacy? I think they are. If so, it is not surprising, for the interest involved in this case is just the sort of interest which the right to privacy typically protects. Since the right that is violated in this case is not also a property right, or a right over the person, the simplifying hypothesis fails. But this should not be surprising, either, for if the right to privacy has a different *point* than these other rights, we should not expect it always to overlap with them. And even if it did always overlap, we could still regard the right to privacy as a distinctive sort of right in virtue of the special kind of interest it protects.

JEFFREY H. REIMAN

Privacy, Intimacy, and Personhood

The Summer 1975 issue of *Philosophy & Public Affairs* featured three articles on privacy, one by Judith Jarvis Thomson, one by Thomas Scanlon in response to Thomson, and one by James Rachels in response to them both.¹ Thomson starts from the observation that “the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is” (p. 295) and goes on to argue that nobody should have one—a very clear idea, that is. Her argument is essentially that all the various protections to which we feel the right to privacy entitles us are already included under other rights, such as “the cluster of rights which the right over the person consists in and also . . . the cluster of rights which owning property consists in” (p. 306). After a romp through some exquisitely fanciful examples, she poses and answers some questions about some of the kinds of “invasions” we would likely think of as violations of the right to privacy:

Someone looks at your pornographic picture in your wall-safe? He violates your right that your belongings not be looked at, and you have that right because you have ownership rights—and it is because you have them that what he does is wrong. Someone uses an

I am grateful to the editors of *Philosophy & Public Affairs* for many helpful comments and suggestions which have aided me in clarifying and communicating the views presented here.

1. Judith Jarvis Thomson, “The Right to Privacy,” Thomas Scanlon, “Thomson on Privacy,” and James Rachels, “Why Privacy is Important,” *Philosophy & Public Affairs* 4, no. 4 (Summer 1975): 295–333. Unless otherwise indicated, page numbers in the text refer to this issue.

X-ray device to look at you through the walls of your house? He violates your right not to be looked at, and you have that right because you have rights over your person analogous to the rights you have over your property—and it is because you have these rights that what he does is wrong [p. 313].

From this she concludes that the right to privacy is “derivative,” and therefore that “there is no need to find the that-which-is-in-common to all rights in the right to privacy cluster and no need to settle disputes about its boundaries” (p. 313). In other words, we are right not to have any very clear idea about what the right is, and we ought not spin our wheels trying to locate some unique “something” that is protected by the right to privacy. Now I think Thomson is wrong about this—and, incidentally, so do Scanlon and Rachels, although I am inclined to believe they think so for the wrong reasons.

Thomson’s argument is a large non sequitur balanced on a small one. She holds that the right to privacy is “derivative” in the sense that each right in the cluster of rights to privacy can be explained by reference to another right and thus without recourse to the right to privacy. This is the little non sequitur. The easiest way to see this is to recognize that it is quite consistent with the notion that the other rights (that is, the rights over one’s person and one’s property) are—in whole or in part—expressions of the right to privacy, and thus *they* are “derivative” from *it*. If all the protections we include under the right to privacy were specified in the Fourth and Fifth Amendments, this would hardly prove that the right to privacy is “derivative” from the right to be secure against unreasonable search or seizure and the privilege against self-incrimination. It would be just as plausible to assert that this is evidence that the Fourth and Fifth Amendment protections are “derivative” from the right to privacy.²

2. This reversibility of “derivative”-ness is to be found in Justice Douglas’ historic opinion on the right to privacy in *Griswold v. State of Connecticut*. He states there that “specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance.” The right of privacy, he goes on to say, is contained in the penumbras of the First, Third, Fourth, Fifth, and Ninth Amendment guarantees. Surely the imagery of penumbral emanations suggests that the right to privacy is “derivative” from the rights protected in these amendments. But later Douglas states that the Court is dealing “with a right of privacy older than the Bill of Rights,”

Now all of this would amount to mere semantics, and Professor Thomson could define "derivative" however she pleased, if she didn't use this as an argument against finding (indeed, against even looking for) the "that-which-is-in-common" to the cluster of rights in the right to privacy. This is the large non sequitur. Even if the right were derivative in the sense urged by Thomson, it would not follow that there is nothing in common to all the protections in the right-to-privacy cluster, or that it would be silly to try to find what they have in common. Criminology is probably derivative from sociology and psychology and law and political science in just the way that Thomson holds privacy rights to be derivative from rights to person and property. This hardly amounts to a reason for not trying to define the unifying theme of criminological studies—at least a large number of criminologists do not think so.³ In other words, even if privacy rights were a grab-bag of property and personal rights, it might still be revealing, as well as helpful, in the resolution of difficult moral conflicts to determine whether there is anything unique that this grab-bag protects that makes it worthy of distinction from the full field of property and personal rights.

I shall argue that there is indeed something unique protected by the right to privacy. And we are likely to miss it if we suppose that what is protected is just a subspecies of the things generally safeguarded by property rights and personal rights. And if we miss it, there may come a time when we think we are merely limiting some personal or property right in favor of some greater good, when in fact we are really sacrificing something of much greater value.

At this point, I shall leave behind all comments on Thomson's paper, since if I am able to prove that there is something unique and uniquely valuable protected by the right to privacy, I shall take this as refutation of her view. It will serve to clarify my own position, however, to indicate briefly what I take to be the shortcomings of the responses of Scanlon and Rachels to Thomson.

which along with other language he uses, suggests that the rights in the Bill of Rights are meant to give reality to an even more fundamental right, the right to privacy. 381 U.S. 479, 85 S. Ct. 1678 (1965).

3. See for instance, Herman and Julia Schwendinger, "Defenders of Order or Guardians of Human Rights?" *Issues in Criminology* 5, no. 2 (Summer 1970): 123-157, especially the section entitled "The Thirty-Year-Old Controversy," pp. 123-129.

Scanlon feels he has refuted Thomson by finding the “special interests” which are the “common foundation” for the right(s) to privacy. He says:

I agree with Thomson that the rights whose violation strikes us as invasion of privacy are many and diverse, and that these rights do not derive from any single overarching right to privacy. I hold, however, that these rights have a common foundation in the special interests that we have in being able to be free from certain kinds of intrusions. The most obvious examples of such offensive intrusions involve observation of our bodies, our behavior or our interactions with other people (or overhearings of the last two), but while these are central they do not exhaust the field [p. 315].

Now on first glance, it is certainly hard to dispute this claim. But it is nonetheless misleading. Scanlon’s position is arresting and appears true because it rests on a tautology, not unlike the classic “explanation” of the capacity of sedatives to induce sleep by virtue of their “dormative powers.” The right to privacy *is* the right “to be free from certain kinds of (offensive) intrusions.” Scanlon’s position is equivalent to holding that the common foundation of our right to privacy lies in our “privatistic interests.”

In sum, Scanlon announces that he has found the common element in rights to privacy: rights to privacy protect our special interest in privacy! Thomson could hardly deny this, although I doubt she would find it adequate to answer the questions she raised in her essay. What Scanlon has not told us is *why* we have a special interest in privacy, that is, a special interest in being free from certain kinds of intrusions; and *why* it is a legitimate interest, that is, an interest of sufficient importance to warrant protection by our fellow citizens.⁴ I suspect that this is the least that would be necessary to convince Thomson that there is a common foundation to privacy rights.

James Rachels tries to provide it. He tries to answer precisely the questions Scanlon leaves unanswered. He asks, “Why, exactly, is privacy important to us?” (p. 323). He starts his answer by categorizing some of the interests we might have in privacy and finds that they

4. I think it is fair to say that Scanlon makes no claim to answer these questions in his essay.

basically have to do with protecting our reputations or the secrecy of our plans or the like. Rachels recognizes, however, that

reflection on these cases gives us little help in understanding the value which privacy has in *normal* or *ordinary* situations. By this I mean situations in which there is nothing embarrassing or shameful or unpopular in what we are doing, and nothing ominous or threatening connected with its possible disclosure. For example, even married couples whose sex-lives are normal (whatever that is), and so who have nothing to be ashamed of, by even the most conventional standards, and certainly nothing to be blackmailed about, do not want their bedrooms bugged [p. 325].

In other words, Rachels recognizes that if there is a unique interest to be protected by the right(s) to privacy, it must be an interest simply in being able to limit other people's observation of us or access to information about us—even if we have certain knowledge that the observation or information would not be used to our detriment or used at all. Rachels tries to identify such an interest and to point out why it is important.

His argument is this. Different human relationships are marked—indeed, in part, constituted—by different degrees of sharing personal information. One shares more of himself with a friend than with an employer, more with a life-long friend than with a casual friend, more with a lover than an acquaintance. He writes that “*however one conceives one's relations with other people, there is inseparable from that conception an idea of how it is appropriate to behave with and around them, and what information about oneself it is appropriate for them to have*” (pp. 328–329). It is “an important part of what it means to have a friend that we welcome his company, that we confide in him, *that we tell him things about ourselves, and that we show him sides of our personalities which we would not tell or show to just anyone*” (pp. 327–328, my emphasis). And therefore, Rachels concludes, “because our ability to control who has access to us, and who knows what about us, allows us to maintain the variety of relationships with other people that we want to have, it is, I think, one of the most important reasons why we value privacy” (p. 329).

Rachels acknowledges that his view is similar to that put forth by

Charles Fried in *An Anatomy of Values*. Since, for our purposes, we can regard these views as substantially the same, and since they amount to an extremely compelling argument about the basis of our interest in privacy, it will serve us well to sample Fried's version of the doctrine. He writes that

privacy is the necessary context for relationships which we would hardly be human if we had to do without—the relationships of love, friendship, and trust.

Love and friendship . . . involve the voluntary and spontaneous relinquishment of something between friend and friend, lover and lover. The title to information about oneself conferred by privacy provides the necessary something. To be friends or lovers persons must be intimate to some degree with each other. Intimacy is the sharing of information about one's actions, beliefs or emotions, which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love.⁵

The Rachels-Fried theory is this. Only because we are able to withhold personal information about—and forbid intimate observation of—ourselves from the rest of the world, can we give out the personal information—and allow the intimate observations—to friends and/or lovers, that constitute intimate relationships. On this view, intimacy is both signaled and constituted by the sharing of information and allowing of observation *not shared with or allowed to the rest of the*

5. Charles Fried, *An Anatomy of Values: Problems of Personal and Social Choice* (Cambridge, Mass., 1970), p. 142. It might be thought that in lifting Fried's analysis of privacy out of his book, I have lifted it out of context and thus done violence to his theory. Extra weight is added to this objection by the recognition that when Fried speaks about love in his book (though not in the chapter relating privacy to love), he speaks of something very like the caring that I present as a basis for refuting his view. For instance Fried writes that, "There is rather a creation of love, a middle term, which is a new pattern or system of interests which both share and both value, in part at least just because it is shared" (*ibid.*, p. 79). What is in conflict between us then is not recognition of this or something like this as an essential component of the love relationship. The conflict rather lies in the fact that I argue that recognition of this factor undermines Fried's claim that *privacy is necessary* for the very existence of love relationships.

world. If there were nothing about myself that the rest of the world did not have access to, I simply would not have anything to give that would mark off a relationship as intimate. As Fried says,

The man who is generous with his possessions, but not with himself, can hardly be a friend, nor—and this more clearly shows the necessity of privacy for love—can the man who, voluntarily or involuntarily, shares everything about himself with the world indiscriminately.⁶

Presumably such a person cannot enter into a friendship or a love because he has literally squandered the “moral capital” which is necessary for intimate emotional investment in another.

Now I find this analysis both compelling and hauntingly distasteful. It is compelling first of all because it fits much that we ordinarily experience. For example, it makes jealousy understandable. If the value—indeed, the very reality—of my intimate relation with you lies in your sharing with me what you don’t share with others, then if you do share it with another, what I have is literally decreased in value and adulterated in substance. This view is also compelling because it meets the basic requirement for identifying a compelling interest at the heart of privacy. That basic requirement is, as I have already stated, an important interest in simply being able to restrict information about, and observation of, myself regardless of what may be done with that information or the results of that observation.

The view is distasteful, however, because it suggests a market conception of personal intimacy. The value and substance of intimacy—like the value and substance of my income—lies not merely in what I have but essentially in what others do *not* have. The reality of my intimacy with you is constituted not simply by the quality and intensity of what we share, but by its unavailability to others—in other words, by its scarcity. It may be that our personal relations are valuable to us because of their exclusiveness rather than because of their own depth or breadth or beauty. But it is not clear that this is necessary. It may be a function of the historical limits of our capacity for empathy and feeling for others. It may be a function of centuries of acculturation

6. *Ibid.*, p. 142.

to the nuclear family with its narrow intensities. The Rachels-Fried thesis, however, makes it into a logical necessity by asserting that friendship and love *logically* imply exclusiveness and narrowness of focus.

As compelling as the Rachels-Fried view is then, there is reason to believe it is an example of the high art of ideology: the rendering of aspects of our present possessive market-oriented world into the eternal forms of logical necessity. Perhaps the tip-off lies precisely in the fact that, on their theory, jealousy—the most possessive of emotions—is rendered rational. All of this is not itself an argument against the Rachels-Fried view, but rather an argument for suspicion. However, it does suggest an argument against that view.

I think the fallacy in the Rachels-Fried view of intimacy is that it overlooks the fact that what constitutes intimacy is not merely the sharing of otherwise withheld information, but the context of caring which makes the sharing of personal information significant. One ordinarily reveals information to one's psychoanalyst that one might hesitate to reveal to a friend or lover. That hardly means one has an intimate relationship with the analyst. And this is not simply because of the asymmetry. If two analysts decided to psychoanalyze one another alternately—the evident unwisdom of this arrangement aside—there is no reason to believe that their relationship would necessarily be the most intimate one in their lives, even if they revealed to each other information they withheld from everyone else, lifelong friends and lovers included. And this wouldn't be changed if they cared about each other's well-being. What is missing is that particular kind of caring that makes a relationship not just personal but intimate.

The kind of caring I have in mind is not easily put in words, and so I shall claim no more than to offer an approximation. Necessary to an intimate relationship such as friendship or love is a reciprocal desire to share present and future intense and important experiences together, not merely to swap information. Mutual psychoanalysis is not love or even friendship so long as it is not animated by this kind of caring. This is why it remains localized in the office rather than tending to spread into other shared activities, as do love and friendship. Were mutual psychoanalysis animated by such caring it might indeed be part of a love or friendship—but then the “prime mover” of

the relationship would not be the exchange of personal information. It would be the caring itself.

In the context of a reciprocal desire to share present and future intense and important experiences, the revealing of personal information takes on significance. The more one knows about the other, the more one is able to understand how the other experiences things, what they mean to him, how they feel to him. In other words the more each knows about the other, the more they are able to really share an intense experience instead of merely having an intense experience alongside one another. The revealing of personal information then is not what constitutes or powers the intimacy. Rather it deepens and fills out, invites and nurtures, the caring that powers the intimacy.

On this view—in contrast to the Rachels-Fried view—it is of little importance who has access to personal information about me. What matters is who cares about it and to whom I care to reveal it. Even if all those to whom I am indifferent and who return the compliment were to know the intimate details of my personal history, my capacity to enter into an intimate relationship would remain unhindered. So long as I could find someone who did not just want to collect data about me, but who cared to know about me in order to share my experience with me and to whom I cared to reveal information about myself so that person could share my experience with me, and vice versa, I could enter into a meaningful friendship or love relationship.

On the Rachels-Fried view, it follows that the significance of sexual intimacy lies in the fact that we signal the uniqueness of our love relationships by allowing our bodies to be seen and touched by the loved one in ways that are forbidden to others. But here too, the context of caring that turns physical contact into intimacy is overlooked. A pair of urologists who examine each other are no more lovers than our reciprocating psychoanalysts. What is missing is the desire to share intense and important experiences. And to say this is to see immediately the appropriateness of sexual intimacy to love: in sexual intimacy one is literally and symbolically stripped of the ordinary masks that obstruct true sharing of experience. This happens not merely in the nakedness of lovers but even more so in the giving of themselves over to the physical forces in their bodies. In surrendering the ordinary restraints, lovers allow themselves to be what they truly

are—at least as bodies—intensely and together. (Recall Sartre’s marvelous description of the *caress*).⁷ If this takes place in the context of caring—in other words if people are making love and not just fucking—their physical intimacy is an expression and a consummation of that caring. It is one form of the authentic speech of loving.

Finally, on this view—in contrast to the Rachels-Fried view—the unsavory market notion of intimacy is avoided. Since the content of intimacy is caring, rather than the revealing of information or the granting of access to the body usually withheld from others, there is no necessary limit to the number of persons one can be intimate with, no logical necessity that friendship or love be exclusive. The limits rather lie in the limits of our capacity to care deeply for others, and of course in the limits of time and energy. In other words it may be a fact—for us at this point in history, or even for all people at all points in history—that we can only enter into a few true friendships and loves in a lifetime. But this is not an inescapable logical necessity. It is only an empirical fact of our capacity, one that might change and might be worth trying to change. It might be a fact that we are unable to disentangle love from jealousy. But this, too, is not an a priori truth. It is rather an empirical fact, one that might change if fortune brought us into a less possessive, less exclusive, less invidious society.

This much is enough, I think, to cast doubt on the relationship between privacy and friendship or love asserted by Rachels and Fried. It should also be enough to refute their theory of the grounds on which the right to privacy rests. For if intimacy *may* be a function of caring and not of the yielding of otherwise withheld information, their claim to have established the *necessity* of privacy for important human relationships must fall. I think, however, that there is another equally

7. “The Other’s flesh did not exist explicitly for me since I grasped the Other’s body in situation; neither did it exist for her since she transcended it toward her possibilities and toward the object. The caress causes the Other to be born as flesh for me and for herself . . . , the caress reveals the flesh by stripping the body of its action, by cutting it off from the possibilities which surround it; the caress is designed to uncover the web of inertia beneath the action—i.e., the pure ‘being-there’—which sustains it. . . . The caress is designed to cause the Other’s body to be born, through pleasure, for the Other—and for myself. . . .” Jean-Paul Sartre, *Being and Nothingness*, trans. Hazel E. Barnes (New York, 1956), p. 390.

fundamental ground for rejecting their position: it makes the right to individual privacy “derivative” from the right to social (that is, interpersonal) relationships. And I mean “derivative” in a much more irreversible way than Thomson does.

On the Rachels-Fried view, my right to parade around naked alone in my house free from observation by human or electronic peeping toms, is not a fundamental right. It is derived from the fact that without this right, I could not meaningfully reveal my body to the loved one in that exclusive way that is necessary to intimacy on the Rachels-Fried view. This strikes me as bizarre. It would imply that a person who had no chance of entering into social relations with others, say a catatonic or a perfectly normal person legitimately sentenced to life imprisonment in solitary confinement, would thereby have no ground for a right to privacy. This must be false, because it seems that if there is a right to privacy it belongs to individuals regardless of whether they are likely to have friends or lovers, regardless of whether they have reason to amass “the moral capital which we spend in friendship and love.” What this suggests is that even if the Rachels-Fried theory of the relationship of privacy and intimacy were true, it would not give us a fundamental interest that can provide the foundation for a right to privacy for all human individuals. I believe, however, that such a fundamental interest can be unearthed. Stanley I. Benn’s theory of the foundation of privacy comes closer to the view which I think is ultimately defensible.

Benn attempts to base the right to privacy on the principle of respect for persons. He too is aware that utilitarian considerations—for example, prevention of harm that may result from misuse of personal information—while important, are not adequate to ground the right to privacy.

The underpinning of a claim not to be watched without leave will be more general if it can be grounded in this way on the principle of respect for persons than on a utilitarian duty to avoid inflicting suffering. That duty may, of course, reinforce the claim in particular instances. But respect for persons will sustain an objection even to secret watching, which may do no actual harm at all. Covert observation—spying—is objectionable because it deliberately

deceives a person about his world [that is, it transforms the situation he thinks is unobserved into one which is observed], thwarting, for reasons that *cannot* be his reasons, his attempts to make a rational choice. One cannot be said to respect a man as engaged on an enterprise worthy of consideration if one knowingly and deliberately alters his conditions of action, concealing the fact from him. The offense is different in this instance, of course, from A's open intrusion on C's conversation. In that case, A's attentions were liable to affect C's enterprise by changing C's perception of it; he may have felt differently about his conversation with D, even to the extent of not being able to see it as any longer the same activity, knowing that A was now listening.⁸

Benn's view is that the right to privacy rests on the principle of respect for persons as choosers. Covert observation or unwanted overt observation deny this respect because they transform the actual conditions in which the person chooses and acts, and thus make it impossible for him to act in the way he set out to act, or to choose in the way he thinks he is choosing.

This too is a compelling analysis. I shall myself argue that the right to privacy is fundamentally connected to personhood. However, as it stands, Benn's theory gives us too much—and though he appears to know it, his way of trimming the theory to manageable scale is not very helpful. Benn's theory gives us too much because it appears to establish a person's right never to be observed when he thought he wasn't being observed, and never to be overtly observed when he didn't wish it. This would give us a right not to have people look at us from their front windows as we absent-mindedly stroll along, as well as a right not to be stared in the face. To deal with this, Benn writes,

it cannot be sufficient that I do not *want* you to observe something; for the principle of respect to be relevant, it must be something about my own person that is in question, otherwise the principle would be so wide that a mere wish of mine would be a *prima facie* reason for everyone to refrain from observing and reporting on anything at all. I do not make something a part of me merely by having feel-

8. Stanley I. Benn, "Privacy, Freedom, and Respect for Persons," in Richard Wasserstrom, ed., *Today's Moral Problems* (New York, 1975), p. 8.

ings about it. The principle of privacy proposed here is, rather, that any man who desires that he *himself* should not be an object of scrutiny has a reasonable claim to immunity.⁹

Benn goes on to say that what is rightly covered by this immunity are one's body and those things, like possessions, which the conventions of a culture may cause one to think of as part of one's identity.

But this begs the question. Benn has moved from the principle that respect for me as a person dictates that I am entitled not to have the conditions in which I choose altered by unknown or unwanted observation, to the principle that I am entitled to have those things (conventionally) bound up with my identity exempt from unknown or unwanted observation. But the first principle does not entail the second, because the second principle is not merely a practical limitation on the first; it is a moral limitation. It asserts that it is wrong (or at least, significantly worse) to have the conditions in which I choose altered, when things closely bound up with my identity are concerned. But this follows only if the first principle is conjoined with another that holds that the closer something is to my identity, the worse it is for others to tamper with it. But this is after all just an abstract version of the right to privacy itself. And since Benn has not shown that it follows from the principle of respect for persons as choosers, his argument presupposes what he seeks to establish. It is quite strictly a *petitio principii*.

In sum then, though we have moved quite a bit further in the direction of the foundation of privacy, we have still not reached our destination. What we are looking for is a fundamental interest, connected to personhood, which provides a basis for a right to privacy to which all human beings are entitled (even those in solitary confinement) and which does not go so far as to claim a right never to be observed (even on crowded streets). I proceed now to the consideration of a candidate for such a fundamental interest.

Privacy is a social practice. It involves a complex of behaviors that stretches from refraining from asking questions about what is none of one's business to refraining from looking into open windows one passes on the street, from refraining from entering a closed door with-

9. *Ibid.*, p. 10.

out knocking to refraining from knocking down a locked door without a warrant.

Privacy can in this sense be looked at as a very complicated social ritual. But what is its point? In response I want to defend the following thesis. *Privacy is a social ritual by means of which an individual's moral title to his existence is conferred.* Privacy is an essential part of the complex social practice by means of which the social group recognizes—and communicates to the individual—that his existence is his own. And this is a precondition of personhood. To be a person, an individual must recognize not just his actual capacity to shape his destiny by his choices. He must also recognize that he has an exclusive moral right to shape his destiny. And this in turn presupposes that he believes that the concrete reality which he is, and through which his destiny is realized, belongs to him in a moral sense.

And if one takes—as I am inclined to—the symbolic interactionist perspective which teaches that “selves” are created in social interaction rather than flowering innately from inborn seeds, to this claim is added an even stronger one: privacy is necessary to the creation of *selves*¹⁰ out of human beings, since a self is at least in part a human being who regards his existence—his thoughts, his body, his actions—as his *own*.

Thus the relationship between privacy and personhood is a twofold one. First, the social ritual of privacy seems to be an essential ingredient in the process by which “persons” are created out of prepersonal infants. It conveys to the developing child the recognition that this body to which he is uniquely “connected” is a body over which he has some exclusive moral rights. Secondly, the social ritual of privacy confirms, and demonstrates respect for, the personhood of already developed persons. I take the notion of “conferring title to one’s existence” to cover both dimensions of the relationship of privacy to personhood: the original bestowal of title and the ongoing confirmation. And of course, to the extent that we believe that the creation of “selves” or “persons” is an ongoing social process—not just something which

10. For purposes of this discussion, we can take “self” and “person” as equivalent. I use them both insofar as they refer to an individual who recognizes that he *owns* his physical and mental reality in the sense that he is morally entitled to realize his destiny through it, and thus that he has at least a strong presumptive moral right not to have others interfere with his self-determination.

occurs once and for all during childhood—the two dimensions become one: privacy is a condition of the original and continuing creation of “selves” or “persons.”

To understand the meaning of this claim, it will be helpful to turn to Erving Goffman’s classic study, “On the Characteristics of Total Institutions.”¹¹ Goffman says of total institutions that “each is a natural experiment on what can be done to the self.”¹² The goal of these experiments is *mortification of the self*, and in each case total deprivation of privacy is an essential ingredient in the regimen. I have taken the liberty of quoting Goffman at length, since I think his analysis provides poignant testimony to the role that elimination of privacy plays in destruction of the self. And thus conversely, he shows the degree to which the self *requires* the social rituals of privacy to exist.

There is another form of mortification in total institutions; beginning with admission a kind of contaminative exposure occurs. On the outside, the individual can hold objects of self-feeling—such as his body, his immediate actions, his thoughts, and some of his possessions—clear of contact with alien and contaminating things. But in total institutions *these territories of the self are violated*. . . .

There is, first, a violation of one’s informational preserve regarding self. During admission, facts about the inmate’s social statuses and past behavior—especially discreditable facts—are collected and recorded in a dossier available to staff. . . .

New audiences not only learn discreditable facts about oneself that are ordinarily concealed but are also in a position to perceive some of these facts directly. Prisoners and mental patients cannot prevent their visitors from seeing them in humiliating circumstances. Another example is the shoulder-patch of ethnic identification worn by concentration-camp inmates. Medical and security examinations often expose the inmate physically, sometimes to persons of both sexes; a similar exposure follows from collective sleeping arrangements and doorless toilets. . . . In general, of course, the inmate is never fully alone; he is always within sight and often earshot of someone, if only his fellow inmates. Prison cages with bars for walls fully realize such exposure.¹³

11. Erving Goffman, *Asylums* (New York, 1961), pp. 1–124.

12. Ibid., p. 12.

13. Ibid., pp. 23–25; my emphasis.

That social practices which penetrate “the private reserve of the individual”¹⁴ are effective means to mortify the inmate’s self—that is, literally, to kill it off—suggests (though it doesn’t prove) that privacy is essential to the creation and maintenance of selves. My argument for this will admittedly be speculative. However, in view of the fact that it escapes the shortcomings of the views we have already analyzed, fits Goffman’s evidence on the effects of deprivation of privacy, fulfills the requirement that it be a fundamental human interest worthy of protection, provides the basis for a right to privacy to which all human beings are entitled, and yet does not claim a right never to be observed, I think it is convincing.

If I am sitting with other people, how do I know this body which is connected to the thoughts I am having is *mine* in the moral sense? That is, how do I know that I have a unique moral right to this body? It is not enough to say that it is connected to my consciousness, since that simply repeats the question or begs the question of what makes these thoughts *my* consciousness. In any event, connection to my consciousness is a factual link, not a moral one. In itself it accounts for why I am not likely to confuse the events in this body (*mine*) with events in that body (*yours*). It does not account for the moral title which gives me a unique right to control the events in this body which I don’t have in respect to the events in that body.

Ownership in the moral sense presupposes a social institution. It is based upon a complex social practice. A social order in which bodies were held to belong to others or to the collectivity, and in which individuals grew up believing that their bodies were not theirs from a moral point of view, is conceivable. To imagine such an order does not require that we deny that for each body only one individual is able to feel or move it. Such a social order is precisely what Goffman portrays in his description of total institutions and it might be thought of as displaying the ultimate logic of totalitarianism. Totalitarianism is the political condition that obtains when a state takes on the characteristics of a total institution. For a society to exist in which individuals do not own their bodies, what is necessary is that people not be treated as if entitled to control what the bodies they can feel and move do, or what is done to those bodies—in particular that they not be treated as if

14. *Ibid.*, p. 29.

entitled to determine when and by whom that body is experienced.¹⁵

This suggests that there are two essential conditions of moral ownership of one's body. The right to do with my body what I wish, and the right to control when and by whom my body is experienced. This in turn reflects the fact that things can be appropriated in two ways: roughly speaking, actively and cognitively. That is, something is "mine" to the extent that I have the power to use it, to dispose of it as I see fit. But additionally there is a way in which something becomes "mine" to the extent that I know it. What I know is "my" knowledge; what I experience is "my" experience. Thus, it follows that if an individual were granted the right to control his bodily movements although always under observation, he might develop some sense of moral ownership of his physical existence.¹⁶ However, that ownership would surely be an impoverished and partial one compared to what we take to be contained in an individual's title to his existence. This is because it would be ownership only in one of the two dimensions of appropriation, the active. Ownership, in the sense we know it, requires control over cognitive appropriation as well. It requires that the individual have control over whether or not his physical existence becomes part of someone else's experience. That is, it requires that the individual be treated as entitled to determine when and by whom his concrete reality is experienced. Moral ownership in the full sense requires the social ritual of privacy.

As I sit among my friends, I know this body is mine because first of all, unlike any other body present, I believe—and my friends have acted and continue to act as if they believe—that I am entitled to do with this body what I wish. Secondly, but also essential, I know this body is mine because unlike any other body present, I have in the past taken it outside of the range of anyone's experience but my own, I can do so now, and I expect to be able to do so in the future. What's more, I believe—and my friends have acted and continue to act as if they

15. Macabre as it may sound, a world in which the body that I can feel and move is *distinct from* the body that I own is conceivable. Imagine, for example, a world of 365 people each born on a different day of the year, in which each person has complete access to the body of the person whose birthday is the day after his.

16. I am indebted to Professor Phillip H. Scribner for pointing this out to me.

believe—that it would be wrong for anyone to interfere with my capacity to do this. In other words, they have and continue to treat me according to the social ritual of privacy. And since my view of myself is, in important ways, a reflection of how others treat me, I come to view myself as the kind of entity that is entitled to the social ritual of privacy. That is, I come to believe that this body is mine in the moral sense.

I think the same thing can be said about the thoughts of which I am aware. That there are thoughts, images, reveries and memories of which only I am conscious does not make them mine in the moral sense—any more than the cylinders in a car belong to it just because they are in it. This is why ascribing ownership of my body to the mere connection with my consciousness begs the question. Ownership of my thoughts requires a social practice as well. It has to do with learning that I can control when, and by whom, the thoughts in my head will be experienced by someone other than myself and learning that I am entitled to such control—that I will not be forced to reveal the contents of my consciousness, even when I put those contents on paper. The contents of my consciousness become mine because they are treated according to the ritual of privacy.

It may seem that this is to return full circle to Thomson's view that the right to privacy is just a species of the rights over person and property. I would argue that it is more fundamental. The right to privacy is the right to the existence of a social practice which makes it possible for me to think of this existence as *mine*. This means that it is the right to conditions necessary for me to think of myself as the kind of entity for whom it would be meaningful and important to claim personal and property rights. It should also be clear that the ownership of which I am speaking is surely more fundamental than property rights. Indeed, it is only when I can call this physical existence mine that I can call objects somehow connected to this physical existence mine. That is, the transformation of physical possession into ownership presupposes ownership of the physical being I am. Thus the right to privacy protects something that is presupposed by both personal and property rights. Thomson's recognition that there is overlap should come as no surprise. The conclusion she draws from the existence of this overlap is, however, unwarranted. Personal and property rights

presuppose an individual with title to his existence—and privacy is the social ritual by which that title is conferred.

The right to privacy, then, protects the individual's interest in becoming, being, and remaining a person. It is thus a right which *all* human individuals possess—even those in solitary confinement. It does not assert a right never to be seen even on a crowded street. It is sufficient that I can control whether and by whom my body is experienced in some significant places and that I have the real possibility of repairing to those places. It is a right which protects my capacity to enter into intimate relations, not because it protects my reserve of generally withheld information, but because it enables me to make the commitment that underlies caring as *my* commitment uniquely conveyed by *my* thoughts and witnessed by *my* actions.

THE END OF FORGETTING

Rosen, Jeffrey

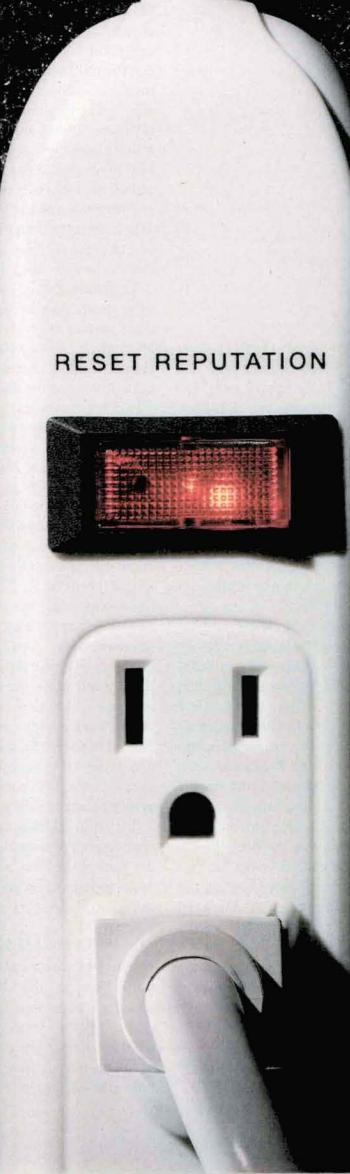
New York Times Magazine; Jul 25, 2010; ProQuest Central
pg. 30

**Legal scholars,
technologists and
cyberthinkers
are wrestling with the
first great
existential crisis of
the digital age:
the impossibility of
erasing your
posted past, starting
over, moving on.**

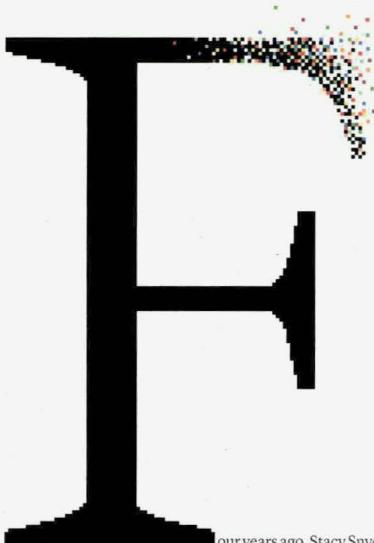
THE END OF FORGETTING

By Jeffrey Rosen

Photo Illustrations by James Wojcik

A close-up photograph of a standard North American electrical outlet. A small, rectangular, glowing red component is attached to the top edge of the outlet. This component has a grid pattern and appears to be a light or a sensor. The outlet itself is white plastic with two vertical slots and one central grounding hole. A white power cord is partially visible, entering from the top left.

RESET REPUTATION



our years ago, Stacy Snyder, then a 25-year-old teacher in training at Conestoga Valley High School in Lancaster, Pa., posted a photo on her MySpace page that showed her at a party wearing a pirate hat and drinking from a plastic cup, with the caption "Drunken Pirate." After discovering the page, her supervisor at the high school told her the photo was "unprofessional," and the dean of Millersville University School of Education, where Snyder was enrolled, said she was promoting drinking in virtual view of her under-age students. As a result, days before Snyder's scheduled graduation, the university denied her a teaching degree. Snyder sued, arguing that the university had violated her First Amendment rights by penalizing her for her (perfectly legal) after-hours behavior. But in 2008, a federal district judge rejected the claim, saying that because Snyder was a public employee whose photo didn't relate to matters of public concern, her "Drunken Pirate" post was not protected speech.

When historians of the future look back on the perils of the early digital age, Stacy Snyder may well be an icon. The problem she faced is only one example of a challenge that, in big and small ways, is confronting millions of people around the globe: how best to live our lives in a world where the Internet records everything and forgets nothing — where every online photo, status update, Twitter post and blog entry by and about us can be stored forever. With Web sites like LOL Facebook Moments, which collects and shares embarrassing personal revelations from Facebook users, ill-advised photos and online chatter are coming back to haunt people months or years after the fact. Examples are proliferating daily: there was the 16-year-old British girl who was fired from her office job for complaining on Facebook, "I'm so totally bored!!"; there was the 66-year-old Canadian psychotherapist who tried to enter the United States but was turned away at the border — and barred permanently from visiting the country — after a border guard's Internet search found that the therapist had written an article in a philosophy journal describing his experiments 30 years ago with L.S.D.

According to a recent survey by Microsoft, 75 percent of U.S. recruiters and human-resource professionals report that their companies require them to do online research about candidates, and many use a range of sites when scrutinizing applicants — including search engines, social-networking sites,

photo- and video-sharing sites, personal Web sites and blogs, Twitter and online-gaming sites. Seventy percent of U.S. recruiters report that they have rejected candidates because of information found online, like photos and discussion-board conversations and membership in controversial groups.

Technological advances, of course, have often presented new threats to privacy. In 1890, in perhaps the most famous article on privacy ever written, Samuel Warren and Louis Brandeis complained that because of new technology — like the Kodak camera and the tabloid press — "gossip is no longer the resource of the idle and of the vicious but has become a trade." But the mild society gossip of the Gilded Age pales before the volume of revelations contained in the photos, video and chatter on social-media sites and elsewhere across the Internet. Facebook, which surpassed MySpace in 2008 as the largest social-networking site, now has nearly 500 million members, or 22 percent of all Internet users, who spend more than 500 billion minutes a month on the site. Facebook users share more than 25 billion pieces of content each month (including news stories, blog posts and photos), and the average user creates 70 pieces of content a month. There are more than 100 million registered Twitter users, and the Library of Congress recently announced that it will be acquiring — and permanently storing — the entire archive of public Twitter posts since 2006.

In Brandeis's day — and until recently, in ours — you had to be a celebrity to be gossiped about in public: today all of us are learning to expect the scrutiny that used to be reserved for the famous and the infamous. A 26-year-old Manhattan woman told *The New York Times* that she was afraid of being tagged in online photos because it might reveal that she wears only two outfit when out on the town — a Lynyrd Skynyrd T-shirt or a basic black dress. "You have movie-star issues," she said, "and you're just a person."

We've known for years that the Web allows for unprecedented voyeurism, exhibitionism and inadvertent indiscretion, but we are only beginning to understand the costs of an age in which so much of what we say, and of what others say about us, goes into our permanent — and public — digital files. The fact that the Internet never seems to forget is threatening, at an almost existential level, our ability to control our identities; to preserve the option of reinventing ourselves and starting anew; to overcome our checkered pasts.

In a recent book, "Delete: The Virtue of Forgetting in the Digital Age," the cyberscholar Viktor Mayer-Schönberger cites Stacy Snyder's case as a reminder of the importance of "societal forgetting." By "erasing external memories," he says in the book, "our society accepts that human beings evolve over time, that we have the capacity to learn from past experiences and adjust our behavior." In traditional societies, where missteps are observed but not necessarily recorded, the limits of human memory ensure that people's sins are eventually forgotten. By contrast, Mayer-Schönberger notes, a society in which everything is recorded "will forever tether us to all our past actions, making it impossible, in practice, to escape them." He concludes that "without some form of forgetting, forgetting becomes a difficult undertaking."

It's often said that we live in a permissive era, one with infinite second chances. But the truth is that for a great many people, the permanent memory bank of the Web increasingly means there are *no* second chances — no opportunities to escape a scarlet letter in your digital past. Now the worst thing you've done is often the first thing everyone knows about you.

THE CRISIS — AND THE SOLUTION?

All this has created something of a collective identity crisis. For most of human history, the idea of reinventing yourself or freely shaping your identity — of presenting different selves in different contexts (at home, at work, at play) — was hard to fathom, because people's identities were fixed by their roles in a rigid social hierarchy. With little geographic or social mobility, you were defined not as an individual but by your village, your class, your job or your guild. But that started to change in the late

Jeffrey Rosen, a law professor at George Washington University, is a frequent contributor to the magazine. He is writing a book about Louis Brandeis.

Middle Ages and the Renaissance, with a growing individualism that came to redefine human identity. As people perceived themselves increasingly as individuals, their status became a function not of inherited categories but of their own efforts and achievements. This new conception of malleable and fluid identity found its fullest and purest expression in the American ideal of the self-made man, a term popularized by Henry Clay in 1832. From the late 18th to the early 20th century, millions of Europeans moved from the Old World to the New World and then continued to move westward across America, a development that led to what the historian Frederick Jackson Turner called "the significance of the frontier," in which the possibility of constant migration from civilization to the wilderness made Americans distrustful of hierarchy and committed to inventing and reinventing themselves.

In the 20th century, however, the ideal of the self-made man came under siege. The end of the Western frontier led to worries that Americans could no longer seek a fresh start and leave their past behind, a kind of reinvention associated with the phrase "G.T.T.," or "Gone to Texas." But the dawning of the Internet age promised to resurrect the ideal of what the psychiatrist Robert Jay Lifton has called the "protean self." If you couldn't flee to Texas, you could always seek out a new chat room and create a new screen name. For some technology enthusiasts, the Web was supposed to be the second flowering of the open frontier, and the ability to segment our identities with an endless supply of pseudonyms, avatars and categories of friendship was supposed to let people present different sides of their personalities in different contexts. What seemed within our grasp was a power that only Proteus possessed: namely, perfect control over our shifting identities.

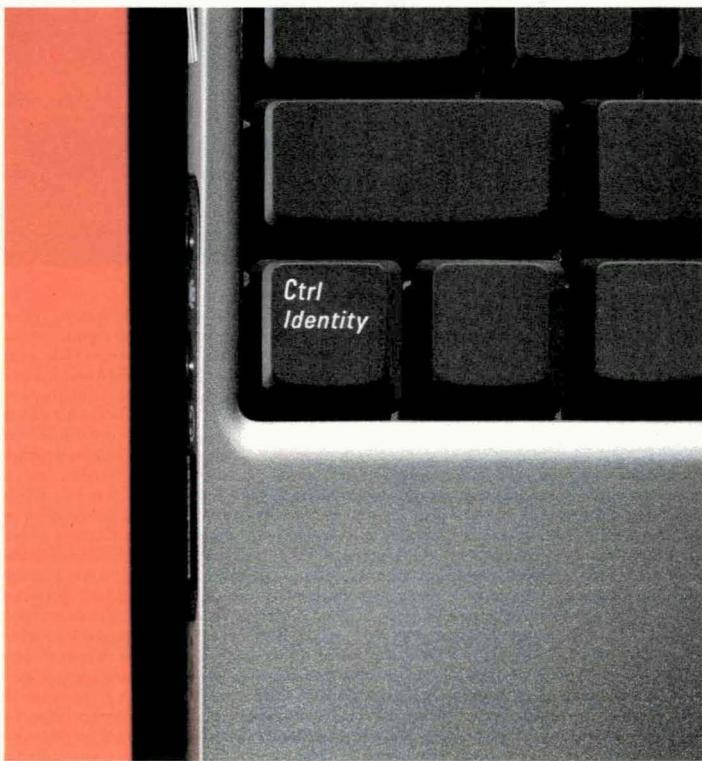
But the hope that we could carefully control how others view us in different contexts has proved to be another myth. As social-networking sites expanded, it was no longer quite so easy to have segmented identities: now that so many people use a single platform to post constant status updates and photos about their private and public activities, the idea of a home self, a work self, a family self and a high-school-friends self has become increasingly untenable. In fact, the attempt to maintain different selves often arouses suspicion. Moreover, far from giving us a new sense of control over the face we present to the world, the Internet is shackling us to everything that we have ever said, or that anyone has said about us, making the possibility of digital self-reinvention seem like an ideal from a distant era.

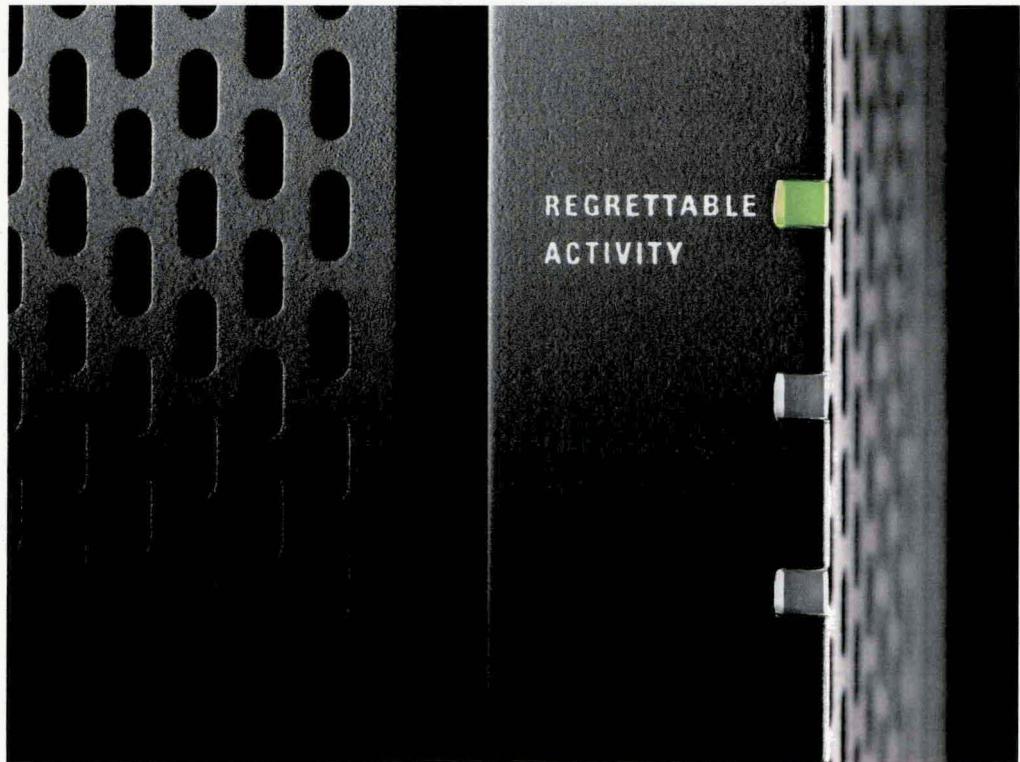
Concern about these developments has intensified this year, as Facebook took steps to make the digital profiles of its users generally more public than private. Last December, the company announced that parts of user profiles that had previously been private — including every user's friends, relationship status and family relations — would become public and accessible to other

users. Then in April, Facebook introduced an interactive system called Open Graph that can share your profile information and friends with the Facebook partner sites you visit.

What followed was an avalanche of criticism from users, privacy regulators and advocates around the world. Four Democratic senators — Charles Schumer of New York, Michael Bennet of Colorado, Mark Begich of Alaska and Al Franken of Minnesota — wrote to the chief executive of Facebook, Mark Zuckerberg, expressing concern about the "instant personalization" feature and the new privacy settings. The reaction to Facebook's changes was such that when four N.Y.U. students announced plans in April to build a free social-networking site called Diaspora, which wouldn't compel users to compromise their privacy, they raised more than \$20,000 from more than 700 backers in a matter of weeks. In May, Facebook responded to all the criticism by introducing a new set of privacy controls that the company said would make it easier for users to understand what kind of information they were sharing in various contexts.

Facebook's partial retreat has not quieted the desire to do something about an urgent problem. All around the world, political leaders, scholars and citizens are searching for responses to the challenge of preserving control of our identities in a digital world that never forgets. Are the most promising solutions going to be technological? Legislative? Judicial? Ethical? A





result of shifting social norms and cultural expectations? Or some mix of the above? Alex Türk, the French data-protection commissioner, has called for a “constitutional right to oblivion” that would allow citizens to maintain a greater degree of anonymity online and in public places. In Argentina, the writers Alejandro Tortolini and Enrique Quagliano have started a campaign to “reinvent forgetting on the Internet,” exploring a range of political and technological ways of making data disappear. In February, the European Union helped finance a campaign called “Think B4 U post!” that urges young people to consider the “potential consequences” of publishing photos of themselves or their friends without “thinking carefully” and asking permission. And in the United States, a group of technologists, legal scholars and cyberthinkers are exploring ways of recreating the possibility of digital forgetting. These approaches share the common goal of reconstructing a form of control over our identities: the ability to reinvent ourselves, to escape our pasts and to improve the selves that we present to the world.

REPUTATION BANKRUPTCY AND TWITTERGATION

A few years ago, at the giddy dawn of the Web 2.0 era — so called to mark the rise of user-generated online content — many technological theorists assumed that self-governing communities could ensure, through the self-correcting wisdom of the crowd, that all participants enjoyed the online identities they deserved. Wikipedia is one embodiment of the faith that the

wisdom of the crowd can correct most mistakes — that a Wikipedia entry for a small-town mayor, for example, will reflect the reputation he deserves. And if the crowd fails — perhaps by turning into a digital mob — Wikipedia offers other forms of redress. Those who think their Wikipedia entries lack context, because they overemphasize a single personal or professional mistake, can petition a group of select editors that decides whether a particular event in someone’s past has been given “undue weight.” For example, if the small-town mayor had an exemplary career but then was arrested for drunken driving, which came to dominate his Wikipedia entry, he can petition to have the event put in context or made less prominent.

In practice, however, self-governing communities like Wikipedia — or algorithmically self-correcting systems like Google — often leave people feeling misrepresented and burned. Those who think that their online reputations have been unfairly tarnished by an isolated incident or two now have a practical option: consulting a firm like ReputationDefender, which promises to clean up your online image. ReputationDefender was founded by Michael Fertik, a Harvard Law School graduate who was troubled by the idea of young people being forever tainted online by their youthful indiscretions. “I was seeing articles about the ‘Lord of the Flies’ behavior that all of us engage in at that age,” he told me, “and it felt un-American that when the conduct was online, it could have permanent effects on the speaker and the victim. The right to new beginnings and the right to self-definition have always been among the most beautiful American ideals.”

ReputationDefender, which has customers in more than 100 countries, is the most successful of the handful of reputation-related start-ups that have been growing rapidly after the privacy concerns raised by Facebook and Google. (ReputationDefender recently raised \$15 million in new venture capital.) For a fee, the company will monitor your online reputation, contacting Web sites individually and asking them to take down offending items. In addition, with the help of the kind of search-optimization technology that businesses use to raise their Google profiles, ReputationDefender can bombard the Web with positive or neutral information about its customers, either creating new Web pages or by multiplying links to existing ones to ensure they show up at the top of any Google search. (Services begin from \$10 a month to \$1,000 a year; for challenging cases, the price can rise into the tens of thousands.) By automatically raising the Google ranks of the positive links, ReputationDefender pushes the negative links to the back pages of a Google search, where they're harder to find. "We're hearing stories of employers increasingly asking candidates to open up Facebook pages in front of them during job interviews," Fertik told me. "Our customers include parents whose kids have talked about them on the Internet — 'Mom didn't get the raise'; 'Dad got fired'; 'Mom and Dad are fighting a lot, and I'm worried they'll get a divorce.'"

Companies like ReputationDefender offer a promising short-term solution for those who can afford it; but tweaking your Google profile may not be enough for reputation management in the near future, as Web 2.0 swiftly gives way to Web 3.0 — a world in which user-generated content is combined with a new layer of data aggregation and analysis and live video. For example, the Facebook application Photo Finder, by Face.com, uses facial-recognition and social-connections software to allow you to locate any photo of yourself or a friend on Facebook, regardless of whether the photo was "tagged" — that is, the individual in the photo was identified by name. At the moment, Photo Finder allows you to identify only people on your contact list, but as facial-recognition technology becomes more widespread and sophisticated, it will almost certainly challenge our expectation of anonymity in public. People will be able to snap a cellphone picture (or video) of a stranger, plug the images into Google and pull up all tagged and untagged photos of that person that exist on the Web.

In the nearer future, Internet searches for images are likely to be combined with social-network aggregator search engines, like today's Spokeo and Pipl, which combine data from online sources — including political contributions, blog posts, YouTube videos, Web comments, real estate listings and photo albums. Increasingly these aggregator sites will rank people's public and private reputations, like the new Web site Unvarnished, a reputation marketplace where people can write anonymous reviews about anyone. In the Web 3.0 world, Fertik predicts, people will be rated, assessed and scored based not on their creditworthiness but on their trustworthiness as good parents, good dates, good employees, good baby sitters or good insurance risks.

Anticipating these challenges, some legal scholars have begun imagining new laws that could allow people to correct, or escape from, the reputation scores that may govern our personal and professional interactions in the future. Jonathan Zittrain, who teaches cyberlaw at Harvard Law School, supports an idea he calls "reputation bankruptcy," which would give people a chance to wipe their reputation slates clean and start over. To illustrate the problem, Zittrain showed me an iPhone app called Date Check,

by Intelius, that offers a "sleaze detector" to let you investigate people you're thinking about dating — it reports their criminal histories, address histories and summaries of their social-networking profiles. Services like Date Check, Zittrain said, could soon become even more sophisticated, rating a person's social desirability based on minute social measurements — like how often he or she was approached or avoided by others at parties (a ranking that would be easy to calibrate under existing technology using cellphones and Bluetooth). Zittrain also speculated that, over time, more and more reputation queries will be processed by a handful of de facto reputation brokers — like the existing consumer-reporting agencies Experian and Equifax, for example — which will provide ratings for people based on their sociability, trustworthiness and employability.

To allow people to escape from negative scores generated by these services, Zittrain says that people should be allowed to declare "reputation bankruptcy" every 10 years or so, wiping out certain categories of ratings or sensitive information. His model is the Fair Credit Reporting Act, which requires consumer-reporting agencies to provide you with one free credit report a year — so you can dispute negative or inaccurate information — and prohibits the agencies from retaining negative information about bankruptcies, late payments or tax liens for more than 10 years. "Like personal financial bankruptcy, or the way in which a state often seals a juvenile criminal record and gives a child a 'fresh start' as an adult," Zittrain writes in his book "The Future of the Internet and How to Stop It," "we ought to consider how to implement the idea of a second or third chance into our digital spaces."

Another proposal, offered by Paul Ohm, a law professor at the University of Colorado, would make it illegal for employers to fire or refuse to hire anyone on the basis of legal off-duty conduct revealed in Facebook postings or Google profiles. "Is it really fair for employers to know what you've put in your Facebook status updates?" Ohm asks. "We could say that Facebook status updates have taken the place of water-cooler chat, which employers were never supposed to overhear, and we could pass a prohibition on the sorts of information employers can and can't consider when they hire someone."

Ohm became interested in this problem in the course of researching the ease with which we can learn the identities of people from supposedly anonymous personal data like movie preferences and health information. When Netflix, for example, released 100 million purportedly anonymous records revealing how almost 500,000 users had rated movies from 1999 to 2005, researchers were able to identify people in the database by name with a high degree of accuracy if they knew even only a little bit about their movie-watching preferences, obtained from public data posted on other ratings sites.

Ohm says he worries that employers would be able to use social-network-aggregator services to identify people's book and movie preferences and even Internet-search terms, and then fire or refuse to hire them on that basis. A handful of states — including New York, California, Colorado and North Dakota — broadly prohibit employers from discriminating against employees for legal off-duty conduct like smoking. Ohm suggests that these laws could be extended to prevent certain categories of employers from refusing to hire people based on Facebook pictures, status updates and other legal but embarrassing personal information. (In practice, these laws might be hard to enforce, since employers might not disclose the real reason for their hiring decisions, so

**The cyberlaw
expert**
**Jonathan Zittrain
says that
the law should
permit people
to declare**

**'REPUTATION
BANKRUPTCY'**
**every 10 years
or so, wiping out
certain
categories of
personal
information
online.**



employers, like credit-reporting agents, might also be required by law to disclose to job candidates the negative information in their digital files.)

Another legal option for responding to online setbacks to your reputation is to sue under current law. There's already a sharp rise in lawsuits known as Twittergation — that is, suits to force Web sites to remove slanderous or false posts. Last year, Courtney Love was sued for libel by the fashion designer Boudoir Queen for supposedly slanderous comments posted on Twitter, on Love's MySpace page and on the designer's online marketplace-feedback page. But even if you win a U.S. libel lawsuit, the Web site doesn't have to take the offending material down any more than a newspaper that has lost a libel suit has to remove the offending content from its archive.

Some scholars, therefore, have proposed creating new legal rights to force Web sites to remove false or slanderous statements. Cass Sunstein, the Obama administration's regulatory czar, suggests in his new book, "On Rumors," that there might be "a general right to demand retraction after a clear demonstration that a statement is both false and damaging." (If a newspaper or blogger refuses to post a retraction, they might be liable for damages.) Sunstein adds that Web sites might be required to take down false postings after receiving notice that they are false — an approach modeled on the Digital Millennium Copyright Act, which requires Web sites to remove content that supposedly infringes intellectual property rights after receiving a complaint.

As Stacy Snyder's "Drunken Pirate" photo suggests, however, many people aren't worried about false information posted by others — they're worried about true information they've posted about themselves when it is taken out of context or given undue weight. And defamation law doesn't apply to true information or statements of opinion. Some legal scholars want to expand the ability to sue over true but embarrassing violations of privacy — although it appears to be a quixotic goal.

Daniel Solove, a George Washington University law professor and author of the book "The Future of Reputation," says that laws forbidding people to breach confidences could be expanded to allow you to sue your Facebook friends if they share your embarrassing photos or posts in violation of your privacy settings. Expanding legal rights in this way, however, would run up against the First Amendment rights of others. Invoking the right to free speech, the U.S. Supreme Court has already held that the media can't be prohibited from publishing the name of a rape victim that they obtained from public records. Generally, American judges hold that if you disclose something to a few people, you can't stop them from sharing the information with the rest of the world.

That's one reason that the most promising solutions to the problem of embarrassing but true information online may be not legal but technological ones. Instead of suing after the damage is done (or hiring a firm to clean up our messes), we need to explore ways of pre-emptively making the offending words or pictures disappear.

EXPIRATION DATES

Jorge Luis Borges, in his short story "Funes, the Memorious," describes a young man who, as a result of a riding accident, has lost his ability to forget. Funes has a tremendous memory, but he is so lost in the details of everything he knows that he is unable to convert the information into knowledge and unable, as a result, to grow in wisdom. Viktor Mayer-Schönberger, in "Delete," uses the Borges story as an emblem for the personal and social costs of being so shackled by our digital past that we

are unable to evolve and learn from our mistakes. After reviewing the various possible legal solutions to this problem, Mayer-Schönberger says he is more convinced by a technological fix: namely, mimicking human forgetting with built-in expiration dates for data. He imagines a world in which digital-storage devices could be programmed to delete photos or blog posts or other data that have reached their expiration dates, and he suggests that users could be prompted to select an expiration date before saving any data.

This is not an entirely fanciful vision. Google not long ago decided to render all search queries anonymous after nine months (by deleting part of each Internet protocol address), and the upstart search engine Cuil has announced that it won't keep any personally identifiable information at all, a privacy feature that distinguishes it from Google. And there are already small-scale privacy apps that offer disappearing data. An app called TigerText allows text-message senders to set a time limit from one minute to 30 days after which the text disappears from the company's servers on which it is stored and therefore from the senders' and recipients' phones. (The founder of TigerText, Jeffrey Evans, has said he chose the name before the scandal involving Tiger Woods's supposed texts to a mistress.)

Expiration dates could be implemented more broadly in various ways. Researchers at the University of Washington, for example, are developing a technology called Vanish that makes electronic data "self-destruct" after a specified period of time. Instead of relying on Google, Facebook or Hotmail to delete the data that is stored "in the cloud" — in other words, on their distributed servers — Vanish encrypts the data and then "shatters" the encryption key. To read the data, your computer has to put the pieces of the key back together, but they "erode" or "rust" as time passes, and after a certain point the document can no longer be read. Tadayoshi Kohno, a designer of Vanish, told me that the system could provide expiration dates not only for e-mail but also for any data stored in the cloud, including photos or text or anything posted on Facebook, Google or blogs. The technology doesn't promise perfect control — you can't stop someone from copying your photos or Facebook chats during the period in which they are not encrypted. But as Vanish improves, it could bring us much closer to a world where our data didn't linger forever.

Kohno told me that Facebook, if it wanted to, could implement expiration dates on its own platform, making our data disappear after, say, three days or three months unless a user specified that he wanted it to linger forever. It might be a more welcome option for Facebook to encourage the development of Vanish-style apps that would allow individual users who are concerned about privacy to make their own data disappear without imposing the default on all Facebook users.

So far, however, Zuckerberg, Facebook's C.E.O., has been moving in the opposite direction — toward transparency rather than privacy. In defending Facebook's recent decision to make the default for profile information about friends and relationship status public rather than private, Zuckerberg said in January to the founder of the publication TechCrunch that Facebook had an obligation to reflect "current social norms" that favored exposure over privacy. "People have really gotten comfortable not only sharing more information and different kinds but more openly and with more people, and that social norm is just something that has evolved over time," he said.

**Researchers
at the University
of Washington
are developing
a technology
called Vanish that
makes
electronic data —
e-mail messages as
well as photos
and text posted
on the Web —**

**'SELF-
DESTRUCT'**
**after a specified
period of time.**



PRIVACY'S NEW NORMAL

But not all Facebook users agree with Zuckerberg. Plenty of anecdotal evidence suggests that young people, having been burned by Facebook (and frustrated by its privacy policy, which at more than 5,000 words is longer than the U.S. Constitution), are savvier than older users about cleaning up their tagged photos and being careful about what they post. And two recent studies challenge the conventional wisdom that young people have no qualms about having their entire lives shared and preserved online forever. A University of California, Berkeley, study released in April found that large majorities of people between 18 and 22 said there should be laws that require Web sites to delete all stored information about individuals (88 percent) and that give people the right to know all the information Web sites know about them (62 percent) — percentages that mirrored the privacy views of older adults. A recent Pew study found that 18-to-29-year-olds are actually more concerned about their online profiles than older people are, vigilantly deleting unwanted posts, removing their names from tagged photos and censoring themselves as they share personal information, because they are coming to understand the dangers of oversharing.

Still, Zuckerberg is on to something when he recognizes that the future of our online identities and reputations will ultimately be shaped not just by laws and technologies but also by changing social norms. And norms are already developing to recreate off-the-record spaces in public, with no photos, Twitter posts or blogging allowed. Milk and Honey, an exclusive bar on Manhattan's Lower East Side, requires potential members to sign an agreement promising not to blog about the bar's goings on or to post photos on social-networking sites, and other bars and nightclubs are adopting similar policies. I've been at dinners recently where someone has requested, in all seriousness, "Please don't tweet this" — a custom that is likely to spread.

But what happens when people transgress those norms, using Twitter or tagging photos in ways that cause us serious embarrassment? Can we imagine a world in which new norms develop that make it easier for people to forgive and forget one another's digital sins?

That kind of social norm may be harder to develop. Alessandro Acquisti, a scholar at Carnegie Mellon University, studies the behavioral economics of privacy — that is, the conscious and unconscious mental trade-offs we make in deciding whether to reveal or conceal information, balancing the benefits of sharing with the dangers of disclosure. He is conducting experiments about the "decay time" and the relative weight of good and bad information — in other words, whether people discount positive information about you more quickly and heavily than they discount negative information about you. His research group's preliminary results suggest that if rumors spread about something good you did 10 years ago, like winning a prize, they will be discounted; but if rumors spread about something bad that you did 10 years ago, like driving drunk, that information has staying power. Research in behavioral psychology confirms that people pay more attention to bad rather than good information, and Acquisti says he fears that "20 years from now, if all of us have a skeleton

ASK THE EXPERTS Michael Fertik, founder of ReputationDefender, and Paul Ohm, a law professor at the University of Colorado, take reader questions on Internet privacy. nytimes.com/magazine



on Facebook, people may not discount it because it was an error in our youth."

On the assumption that strangers may not make it easy for us to escape our pasts, Acquisti is also studying technologies and strategies of "privacy nudges" that might prompt people to think twice before sharing sensitive photos or information in the first place. Gmail, for example, has introduced a feature that forces you to think twice before sending drunken e-mail messages. When you enable the feature, called Mail Goggles, it prompts you to solve simple math problems before sending e-mail messages at times you're likely to regret. (By default, Mail Goggles is active only late on weekend nights.) Acquisti is investigating similar strategies of "soft paternalism" that might nudge people to hesitate before posting, say, drunken photos from Cancún. "We could easily think about a system, when you are uploading certain photos, that immediately detects how sensitive the photo will be."

A silly but surprisingly effective alternative might be to have an anthropomorphic icon — a stern version of Microsoft's Clippy — that could give you a reproachful look before you hit the send button. According to M. Ryan Calo, who runs the consumer-privacy project at Stanford Law School, experimenters studying strategies of "visceral notice" have found that when people navigate a Web site in the presence of a human-looking online character who seems to be actively following. (Continued on Page 44)

PRIVACY

(Continued from Page 37)

the cursor, they disclose less personal information than people who browse with no character or one who appears not to be paying attention. As people continue to experience the drawbacks of living in a world that never forgets, they may well learn to hesitate before posting information, with or without humanoid Clippy.

FORGIVENESS

In addition to exposing less for the Web to forget, it might be helpful for us to explore new ways of living in a world that is slow to forgive. It's sobering, now that we live in a world misleadingly called a "global village," to think about privacy in actual, small villages long ago. In the villages described in the Babylonian Talmud, for example, any kind of gossip or tale-bearing about other people — oral or written, true or false, friendly or mean — was considered a terrible sin because small communities have long memories and every word spoken about other people was thought to

ascend to the heavenly cloud. (The digital cloud has made this metaphor literal.) But the Talmudic villages were, in fact, far more humane and forgiving than our brutal global village, where much of the content on the Internet would meet the Talmudic definition of gossip: although the Talmudic sages believed that God reads our thoughts and records them in the book of life, they also believed that God erases the book for those who atone for their sins by asking forgiveness of those they have wronged. In the Talmud, people have an obligation not to remind others of their past misdeeds, on the assumption they may have atoned and grown spiritually from their mistakes. "If a man was a repentant [sinner]," the Talmud says, "one must not say to him, 'Remember your former deeds...'"

Unlike God, however, the digital cloud rarely wipes our slates clean, and the keepers of the cloud today are sometimes less forgiving than their all-powerful divine predecessor. In an interview with Charlie Rose on PBS, Eric Schmidt, the

C.E.O. of Google, said that “the next generation is infinitely more social online” — and less private — “as evidenced by their Facebook pictures,” which “will be around when they’re running for president years from now.” Schmidt added: “As long as the answer is that I chose to make a mess of myself with this picture, then it’s fine. The issue is when somebody else does it.” If people choose to expose themselves for 15 minutes of fame, Schmidt says, “that’s their choice, and they have to live with it.”

Schmidt added that the "notion of control is fundamental to the evolution of these privacy-based solutions," pointing to Google Latitude, which allows people to broadcast their locations in real time.

This idea of privacy as a form of control is echoed by many privacy scholars, but it seems too harsh to say that if people like Stacy Snyder don't use their privacy settings responsibly, they have to live forever with the consequences. Privacy protects us from being unfairly judged out of context on the basis of snippets of private information that

have been exposed against our will; but we can be just as unfairly judged out of context on the basis of snippets of public information that we have unwisely chosen to reveal to the wrong audience.

Moreover, the narrow focus on privacy as a form of control misses what really worries people on the Internet today. What people seem to want is not simply control over their privacy settings; they want control over their online reputations. But the idea that any of us can control our reputations is, of course, an unrealistic fantasy. The truth is we can't possibly control what others say or know or think about us in a world of Facebook and Google, nor can we realistically demand that others give us the deference and respect to which we think we're entitled. On the Internet, it turns out, we're not entitled to demand any particular respect at all, and if others don't have the empathy necessary to forgive our missteps, or the attention spans necessary to judge us in context, there's nothing we can do about it.

DIAGRAMLESS

BY FRED PISCOP

This diagramless crossword is 17 squares wide by 17 squares deep and has regular crossword symmetry.
The first square across is given with last week's answers.

ACROSS		DOWN	
I	500 sheets	49 "Go team!"	7 Fish in a garden pool
5	2010 N.B.A. champs	51 Floored the accelerator	8 Medevac destinations, briefly
II	Melvin known as the King of Torts	55 Cote sound	9 Talk like a tough guy
12	Lacking principles	57 Touched up	10 Turn on a pivot
13	Equivocated	58 Campaign fund	11 Keeps occupied
16	Morale-boosting grp.	61 Keep watch over	13 Boneheaded
17	Deck out	62 Where shepherds keep watch	14 Holy scroll
18	Study intently	63 Vacation rental	15 Fished with pots
22	Orbiter until 2001	64 Bars, legally	19 Attention to detail
23	Camera type, for short	67 Fresh-mouthed	20 Present a case
24	Trevi toss-in, once	69 Sit in a cellar, say	21 "Mmm-mm-good!"
25	Bunk framework	70 Dried out quickly	26 Listing in a how-to
28	Rotten so-and-sos	74 Of a main line	27 Talk show talk
31	Command after "ready"	75 Old-time politico Kefauver	28 Go all-in, say
32	Turned yellow	76 Fancy-shmancy	29 Quotation book abbr.
35	State on a bay: Abbr.	77 1.0 equivalents	30 Put on the shelf
37	Countless		33 Mild smoke
38	Actor Alejandro or Fernando	1 Made a tape of	34 Act the bootlicker
39	Young seal	2 Bugling beast	36 Like tabloid headlines
41	11-Across's profession	3 The Rays' div.	40 Best of the early Beatles
42	Earn	4 Piano student's reference point	43 Dash gadget
44	Schooner filler	5 Co-star of Haley and Bolger	44 Playground shooter
47	Big bang	6 Call from the flock	45 Causes to limp
			46 Triple jump, e.g.
DOWN			
			48 Add to dishonestly
			50 Cornmeal concoctions
			52 Fund
			53 "To your health!"
			54 Put up
			56 Siouan speakers
			59 Oregon Indian
			60 Deuce beater
			65 Wasabi __ (spicy snack)
			66 Rare cause of April baseball postponements
			67 Overcharge, slangily
			68 On your side
			71 Lifting syllable
			72 UPS unit: Abbr.
			73 66, famously: Abbr.

BOYS' BOARDING

Your son will
succeed.



St. Thomas More School

- Renowned college preparatory boarding school for young men who have not yet realized their potential
- Located in scenic southeastern Connecticut
- stmct.org
860.823.3861

SHOPPING @ HOME

Cafe Daum. Michael Thonet's Model #4 is one of his earliest designs. This sexy, curvy beauty is still made in Poland's original factory, hand-caned and steam bent in the old, traditional way. Black or natural, with natural cane. Side Chair \$239

\$269 homeward

National Ordering 800-616-3667
Fox 202-526-5679 FAX 202-526-5111 M-F 9AM-5PM • VISA • MC • AE
www.homewardfurniture.com • Shipping

17

**Think
Inside
The Box**

Join
The New York Times
Crossword Society

25

One-year membership,
\$49.95
Call 1-888-7ACROSS
(1-888-722-7677)

The New York Times

CROSSWORD SOCIETY

www.nytimes.com/crossword

But if we can't control what others think or say or view about us, we can control our own reaction to photos, videos, blogs and Twitter posts that we feel unfairly represent us. A recent study suggests that people on Facebook and other social-networking sites express their real personalities, despite the widely held assumption that people try online to express an enhanced or idealized impression of themselves. Samuel Gosling, the University of Texas, Austin, psychology professor who conducted the study, told the Facebook blog, "We found that judgments of people based on nothing but their Facebook profiles correlate pretty strongly with our measure of what that person is really like, and that measure consists of both how the profile owner sees him or herself and how that profile owner's friends see the profile owner."

By comparing the online profiles of college-aged people in the United States and Germany with their

actual personalities and their idealized personalities, or how they wanted to see themselves, Gosling found that the online profiles conveyed "rather accurate images of the profile owners, either because people aren't trying to look good or because they are trying and failing to pull it off." (Personality impressions based on the online profiles were most accurate for extroverted people and least accurate for neurotic people, who cling tenaciously to an idealized self-image.)

Gosling is optimistic about the implications of his study for the possibility of digital forgiveness. He acknowledged that social technologies are forcing us to merge identities that used to be separate — we can no longer have segmented selves like "a home or family self, a friend self, a leisure self, a work self." But although he told Facebook, "I have to find a way to reconcile my professor self with my having-a-few-drinks self," he also suggested that as all of us have to merge our public and private identities, photos showing us having a few drinks on Facebook will no longer seem so scandalous. "You see your accountant going out on weekends and attending clown conventions, that no longer makes you think that he's not a good accountant. We're coming to terms and reconciling with that merging of identities."

Perhaps society will become more forgiving of drunken Facebook pictures in the way Gosling says he expects it might. And some may welcome the end of the segmented self, on the grounds that it will discourage bad behavior and hypocrisy: it's harder to have clandestine affairs when you're broadcasting your every move on Facebook, Twitter and Four-square. But a humane society values privacy, because it allows people to cultivate different aspects of their personalities in different contexts; and at the moment, the enforced merging of identities that used to be separate is leaving many casualties in its wake. Stacy Snyder couldn't reconcile her "aspiring-teacher self" with her "having-a-few-drinks self"; even the impression, correct or not, that she had a drink in a pirate hat at an off-campus party was enough to derail her teaching career.

That doesn't mean, however, that it had to derail her life. After taking down her MySpace profile, Snyder is understandably trying to maintain her privacy: her lawyer told me in a recent interview that she is now working in human resources; she did not respond to a request for comment. But her success as a human being who can change and evolve, learning from her mistakes and growing in wisdom, has nothing to do with the digital file she can never entirely escape. Our character, ultimately, can't be judged by strangers on the basis of our Facebook or Google profiles; it can be judged by only those who know us and have time to evaluate our strengths and weaknesses, face to face and in context, with insight and understanding. In the meantime, as all of us stumble over the challenges of living in a world without forgetting, we need to learn new forms of empathy, new ways of defining ourselves without reference to what others say about us and new ways of forgiving one another for the digital trails that will follow us forever. ♦

ANSWERS TO PUZZLES OF 7.18.10
Critical Periods



RICHARD FURNALD SMITH, PRELUDE TO SCIENCE —
Most chemists are tolerant — even proud — about alchemy, but astronomers take a hard line toward astrology. Possibly chemists would be less broadminded if they ... saw columns of alchemical advice in all the daily newspapers.

- | | | |
|-------------|---------------|--------------|
| A. Reformed | I. Rhapsodic | Q. Satiate |
| B. Feelers | J. Embolden | R. Corn dog |
| C. Synopsis | K. Limestone | S. Islamabad |
| D. Muscatel | L. Unbowed | T. Ellsworth |
| E. Idolatry | M. Decathlon | U. Numbat |
| F. Tribunal | N. Ecosystem | V. Chivalry |
| G. Hacksaw | O. Test-drive | W. Elisha |
| H. Put away | P. Omphalos | |

NOTE: 1-Across in this week's diagramless puzzle begins in the 3rd square of the top row.

Syllabus

SMITH v. MARYLAND

CERTIORARI TO THE COURT OF APPEALS OF MARYLAND

No. 78-5374. Argued March 28, 1979—Decided June 20, 1979

The telephone company, at police request, installed at its central offices a pen register to record the numbers dialed from the telephone at petitioner's home. Prior to his robbery trial, petitioner moved to suppress "all fruits derived from" the pen register. The Maryland trial court denied this motion, holding that the warrantless installation of the pen register did not violate the Fourth Amendment. Petitioner was convicted, and the Maryland Court of Appeals affirmed.

Held: The installation and use of the pen register was not a "search" within the meaning of the Fourth Amendment, and hence no warrant was required. Pp. 739-746.

(a) Application of the Fourth Amendment depends on whether the person invoking its protection can claim a "legitimate expectation of privacy" that has been invaded by government action. This inquiry normally embraces two questions: first, whether the individual has exhibited an actual (subjective) expectation of privacy; and second, whether his expectation is one that society is prepared to recognize as "reasonable." *Katz v. United States*, 389 U. S. 347. Pp. 739-741.

(b) Petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and even if he did, his expectation was not "legitimate." First, it is doubtful that telephone users in general have any expectation of privacy regarding the numbers they dial, since they typically know that they must convey phone numbers to the telephone company and that the company has facilities for recording this information and does in fact record it for various legitimate business purposes. And petitioner did not demonstrate an expectation of privacy merely by using his home phone rather than some other phone, since his conduct, although perhaps calculated to keep the *contents* of his conversation private, was not calculated to preserve the privacy of the number he dialed. Second, even if petitioner did harbor some subjective expectation of privacy, this expectation was not one that society is prepared to recognize as "reasonable." When petitioner voluntarily conveyed numerical information to the phone company and "exposed" that information to its equipment in the normal course of business, he assumed the risk that the company would reveal the infor-

Opinion of the Court

442 U.S.

mation to the police, cf. *United States v. Miller*, 425 U. S. 435. Pp. 741-746.
283 Md. 156, 389 A. 2d 858, affirmed.

BLACKMUN, J., delivered the opinion of the Court, in which BURGER, C. J., and WHITE, REHNQUIST, and STEVENS, JJ., joined. STEWART, J., post, p. 746, and MARSHALL, J., post, p. 748, filed dissenting opinions, in which BRENNAN, J., joined. POWELL, J., took no part in the consideration or decision of the case.

Howard L. Cardin argued the cause for petitioner. With him on the brief was *James J. Gitomer*.

Stephen H. Sachs, Attorney General of Maryland, argued the cause for respondent. With him on the brief were *George A. Nilson*, Deputy Attorney General, and *Deborah K. Handel* and *Stephen B. Caplis*, Assistant Attorneys General.

MR. JUSTICE BLACKMUN delivered the opinion of the Court.

This case presents the question whether the installation and use of a pen register¹ constitutes a "search" within the meaning of the Fourth Amendment,² made applicable to the States through the Fourteenth Amendment. *Mapp v. Ohio*, 367 U. S. 643 (1961).

¹ "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." *United States v. New York Tel. Co.*, 434 U. S. 159, 161 n. 1 (1977). A pen register is "usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line" to which it is attached. *United States v. Giordano*, 416 U. S. 505, 549 n. 1 (1974) (opinion concurring in part and dissenting in part). See also *United States v. New York Tel. Co.*, 434 U. S., at 162.

² "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U. S. Const., Amdt. 4.

I

On March 5, 1976, in Baltimore, Md., Patricia McDonough was robbed. She gave the police a description of the robber and of a 1975 Monte Carlo automobile she had observed near the scene of the crime. Tr. 66-68. After the robbery, McDonough began receiving threatening and obscene phone calls from a man identifying himself as the robber. On one occasion, the caller asked that she step out on her front porch; she did so, and saw the 1975 Monte Carlo she had earlier described to police moving slowly past her home. *Id.*, at 70. On March 16, police spotted a man who met McDonough's description driving a 1975 Monte Carlo in her neighborhood. *Id.*, at 71-72. By tracing the license plate number, police learned that the car was registered in the name of petitioner, Michael Lee Smith. *Id.*, at 72.

The next day, the telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at petitioner's home. *Id.*, at 73, 75. The police did not get a warrant or court order before having the pen register installed. The register revealed that on March 17 a call was placed from petitioner's home to McDonough's phone. *Id.*, at 74. On the basis of this and other evidence, the police obtained a warrant to search petitioner's residence. *Id.*, at 75. The search revealed that a page in petitioner's phone book was turned down to the name and number of Patricia McDonough; the phone book was seized. *Ibid.* Petitioner was arrested, and a six-man lineup was held on March 19. McDonough identified petitioner as the man who had robbed her. *Id.*, at 70-71.

Petitioner was indicted in the Criminal Court of Baltimore for robbery. By pretrial motion, he sought to suppress "all fruits derived from the pen register" on the ground that the police had failed to secure a warrant prior to its installation. Record 14; Tr. 54-56. The trial court denied the suppression motion, holding that the warrantless installation of the pen

Opinion of the Court

442 U.S.

register did not violate the Fourth Amendment. *Id.*, at 63. Petitioner then waived a jury, and the case was submitted to the court on an agreed statement of facts. *Id.*, at 65-66. The pen register tape (evidencing the fact that a phone call had been made from petitioner's phone to McDonough's phone) and the phone book seized in the search of petitioner's residence were admitted into evidence against him. *Id.*, at 74-76. Petitioner was convicted, *id.*, at 78, and was sentenced to six years. He appealed to the Maryland Court of Special Appeals, but the Court of Appeals of Maryland issued a writ of certiorari to the intermediate court in advance of its decision in order to consider whether the pen register evidence had been properly admitted at petitioner's trial. 283 Md. 156, 160, 389 A. 2d 858, 860 (1978).

The Court of Appeals affirmed the judgment of conviction, holding that "there is no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system and hence no search within the fourth amendment is implicated by the use of a pen register installed at the central offices of the telephone company." *Id.*, at 173, 389 A. 2d, at 867. Because there was no "search," the court concluded, no warrant was needed. Three judges dissented, expressing the view that individuals do have a legitimate expectation of privacy regarding the phone numbers they dial from their homes; that the installation of a pen register thus constitutes a "search"; and that, in the absence of exigent circumstances, the failure of police to secure a warrant mandated that the pen register evidence here be excluded. *Id.*, at 174, 178, 389 A. 2d, at 868, 870. Certiorari was granted in order to resolve indications of conflict in the decided cases as to the restrictions imposed by the Fourth Amendment on the use of pen registers.³ 439 U. S. 1001 (1978).

³ See *Application of United States for Order*, 546 F. 2d 243, 245 (CA8 1976), cert. denied *sub nom. Southwestern Bell Tel. Co. v. United States*, 434 U. S. 1008 (1978); *Application of United States in Matter of Order*,

II

A

The Fourth Amendment guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” In determining whether a particular form of government-initiated electronic surveillance is a “search” within the meaning of the Fourth Amendment,⁴ our lodestar is *Katz v. United States*, 389 U. S. 347 (1967). In *Katz*, Government agents had intercepted the contents of a telephone conversation by attaching an electronic listening device to the outside of a public phone booth. The Court rejected the argument that a “search” can occur only when there has been a “physical intrusion” into a “constitutionally protected area,” noting that the Fourth Amendment “protects people, not places.” *Id.*, at 351–353. Because the Government’s monitoring of Katz’ conversation “violated the privacy upon which he justifiably relied while using the telephone booth,” the Court held that

538 F. 2d 956, 959–960 (CA2 1976), rev’d on other grounds *sub nom. United States v. New York Tel. Co.*, 434 U. S. 159 (1977); *United States v. Falcone*, 505 F. 2d 478, 482, and n. 21 (CA3 1974), cert. denied, 420 U. S. 955 (1975); *Hodge v. Mountain States Tel. & Tel. Co.*, 555 F. 2d 254, 256 (CA9 1977); *id.*, at 266 (concurring opinion); and *United States v. Clegg*, 509 F. 2d 605, 610 (CA5 1975). In previous decisions, this Court has not found it necessary to consider whether “pen register surveillance [is] subject to the requirements of the Fourth Amendment.” *United States v. New York Tel. Co.*, 434 U. S., at 165 n. 7. See *United States v. Giordano*, 416 U. S., at 554 n. 4 (opinion concurring in part and dissenting in part).

⁴ In this case, the pen register was installed, and the numbers dialed were recorded, by the telephone company. Tr. 73–74. The telephone company, however, acted at police request. *Id.*, at 73, 75. In view of this, respondent appears to concede that the company is to be deemed an “agent” of the police for purposes of this case, so as to render the installation and use of the pen register “state action” under the Fourth and Fourteenth Amendments. We may assume that “state action” was present here.

Opinion of the Court

442 U. S.

it "constituted a 'search and seizure' within the meaning of the Fourth Amendment." *Id.*, at 353.

Consistently with *Katz*, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a "justifiable," a "reasonable," or a "legitimate expectation of privacy" that has been invaded by government action. *E. g., Rakas v. Illinois*, 439 U. S. 128, 143, and n. 12 (1978); *id.*, at 150, 151 (concurring opinion); *id.*, at 164 (dissenting opinion); *United States v. Chadwick*, 433 U. S. 1, 7 (1977); *United States v. Miller*, 425 U. S. 435, 442 (1976); *United States v. Dionisio*, 410 U. S. 1, 14 (1973); *Couch v. United States*, 409 U. S. 322, 335-336 (1973); *United States v. White*, 401 U. S. 745, 752 (1971) (plurality opinion); *Mancusi v. DeForte*, 392 U. S. 364, 368 (1968); *Terry v. Ohio*, 392 U. S. 1, 9 (1968). This inquiry, as Mr. Justice Harlan aptly noted in his *Katz* concurrence, normally embraces two discrete questions. The first is whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy," 389 U. S., at 361—whether, in the words of the *Katz* majority, the individual has shown that "he seeks to preserve [something] as private." *Id.*, at 351. The second question is whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable,'" *id.*, at 361—whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is "justifiable" under the circumstances. *Id.*, at 353.⁵ See *Rakas v. Illinois*, 439 U. S.,

⁵ Situations can be imagined, of course, in which *Katz'* two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding

at 143–144, n. 12; *id.*, at 151 (concurring opinion); *United States v. White*, 401 U. S., at 752 (plurality opinion).

B

In applying the *Katz* analysis to this case, it is important to begin by specifying precisely the nature of the state activity that is challenged. The activity here took the form of installing and using a pen register. Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner obviously cannot claim that his "property" was invaded or that police intruded into a "constitutionally protected area." Petitioner's claim, rather, is that, notwithstanding the absence of a trespass, the State, as did the Government in *Katz*, infringed a "legitimate expectation of privacy" that petitioner held. Yet a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications. This Court recently noted:

"Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."

United States v. New York Tel. Co., 434 U. S. 159, 167 (1977).

the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.

Opinion of the Court

442 U.S.

Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a "search" necessarily rests upon a claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone.

This claim must be rejected. First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies "for the purposes of checking billing operations, detecting fraud, and preventing violations of law." *United States v. New York Tel. Co.*, 434 U. S., at 174-175. Electronic equipment is used not only to keep billing records of toll calls, but also "to keep a record of all calls dialed from a telephone which is subject to a special rate structure." *Hodge v. Mountain States Tel. & Tel. Co.*, 555 F. 2d 254, 266 (CA9 1977) (concurring opinion). Pen registers are regularly employed "to determine whether a home phone is being used to conduct a business, to check for a defective dial, or to check for overbilling." Note, The Legal Constraints upon the Use of the Pen Register as a Law Enforcement Tool, 60 Cornell L. Rev. 1028, 1029 (1975) (footnotes omitted). Although most people may be oblivious to a pen register's esoteric functions, they presumably have some awareness of one common use: to aid in the identification of persons making annoying or obscene calls. See, e. g., *Von Lusch v. C & P Telephone Co.*, 457 F. Supp. 814, 816 (Md. 1978); Note, 60 Cornell L. Rev., at 1029-1030, n. 11; Claerhout, The Pen Register, 20 Drake L. Rev. 108, 110-111 (1970). Most phone books tell

subscribers, on a page entitled "Consumer Information," that the company "can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls." *E. g.*, Baltimore Telephone Directory 21 (1978); District of Columbia Telephone Directory 13 (1978). Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.

Petitioner argues, however, that, whatever the expectations of telephone users in general, he demonstrated an expectation of privacy by his own conduct here, since he "us[ed] the telephone *in his house* to the exclusion of all others." Brief for Petitioner 6 (emphasis added). But the site of the call is immaterial for purposes of analysis in this case. Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would.

Second, even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not "one that society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U. S., at 361. This Court consistently has held that a person has no legitimate expectation of privacy in information he

Opinion of the Court

442 U.S.

voluntarily turns over to third parties. *E. g., United States v. Miller*, 425 U. S., at 442-444; *Couch v. United States*, 409 U. S., at 335-336; *United States v. White*, 401 U. S., at 752 (plurality opinion); *Hoffa v. United States*, 385 U. S. 293, 302 (1966); *Lopez v. United States*, 373 U. S. 427 (1963). In *Miller*, for example, the Court held that a bank depositor has no "legitimate 'expectation of privacy'" in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business." 425 U. S., at 442. The Court explained:

"The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.*, at 443.

Because the depositor "assumed the risk" of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private.

This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. Tr. of Oral Arg. 3-5, 11-12, 32. We

are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.

Petitioner argues, however, that automatic switching equipment differs from a live operator in one pertinent respect. An operator, in theory at least, is capable of remembering every number that is conveyed to him by callers. Electronic equipment, by contrast, can "remember" only those numbers it is programmed to record, and telephone companies, in view of their present billing practices, usually do not record local calls. Since petitioner, in calling McDonough, was making a local call, his expectation of privacy as to her number, on this theory, would be "legitimate."

This argument does not withstand scrutiny. The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not, in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be divulged to police. Under petitioner's theory, Fourth Amendment protection would exist, or not, depending on how the telephone company chose to define local-dialing zones, and depending on how it chose to bill its customers for local calls. Calls placed across town, or dialed directly, would be protected; calls placed across the river, or dialed with operator assistance, might not be. We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.

We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not "legitimate." The installation and use of a pen reg-

STEWART, J., dissenting

442 U.S.

ister, consequently, was not a "search," and no warrant was required. The judgment of the Maryland Court of Appeals is affirmed.

It is so ordered.

MR. JUSTICE POWELL took no part in the consideration or decision of this case.

MR. JUSTICE STEWART, with whom MR. JUSTICE BRENNAN joins, dissenting.

I am not persuaded that the numbers dialed from a private telephone fall outside the constitutional protection of the Fourth and Fourteenth Amendments.

In *Katz v. United States*, 389 U. S. 347, 352, the Court acknowledged the "vital role that the public telephone has come to play in private communication[s]." The role played by a private telephone is even more vital, and since *Katz* it has been abundantly clear that telephone conversations carried on by people in their homes or offices are fully protected by the Fourth and Fourteenth Amendments. As the Court said in *United States v. United States District Court*, 407 U. S. 297, 313, "the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." (Footnote omitted.)

Nevertheless, the Court today says that those safeguards do not extend to the numbers dialed from a private telephone, apparently because when a caller dials a number the digits may be recorded by the telephone company for billing purposes. But that observation no more than describes the basic nature of telephone calls. A telephone call simply cannot be made without the use of telephone company property and without payment to the company for the service. The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we

have squarely held that the user of even a public telephone is entitled "to assume that the words he utters into the mouth-piece will not be broadcast to the world." *Katz v. United States, supra*, at 352.

The central question in this case is whether a person who makes telephone calls from his home is entitled to make a similar assumption about the numbers he dials. What the telephone company does or might do with those numbers is no more relevant to this inquiry than it would be in a case involving the conversation itself. It is simply not enough to say, after *Katz*, that there is no legitimate expectation of privacy in the numbers dialed because the caller assumes the risk that the telephone company will disclose them to the police.

I think that the numbers dialed from a private telephone—like the conversations that occur during a call—are within the constitutional protection recognized in *Katz*.¹ It seems clear to me that information obtained by pen register surveillance of a private telephone is information in which the telephone subscriber has a legitimate expectation of privacy.² The information captured by such surveillance emanates from private conduct within a person's home or office—locations that without question are entitled to Fourth and Fourteenth Amendment protection. Further, that information is an integral part of the telephonic communication that under *Katz*

¹ It is true, as the Court pointed out in *United States v. New York Tel. Co.*, 434 U. S. 159, 166-167, that under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U. S. C. §§ 2510-2520, pen registers are not considered "interceptions" because "they do not acquire the 'contents' of communications," as that term is defined by Congress. We are concerned in this case, however, not with the technical definitions of a statute, but with the requirements of the Constitution.

² The question whether a defendant who is not a member of the subscriber's household has "standing" to object to pen register surveillance of a private telephone is, of course, distinct. Cf. *Rakas v. Illinois*, 439 U. S. 128.

MARSHALL, J., dissenting

442 U.S.

is entitled to constitutional protection, whether or not it is captured by a trespass into such an area.

The numbers dialed from a private telephone—although certainly more prosaic than the conversation itself—are not without “content.” Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person’s life.

I respectfully dissent.

MR. JUSTICE MARSHALL, with whom MR. JUSTICE BRENNAN joins, dissenting.

The Court concludes that because individuals have no actual or legitimate expectation of privacy in information they voluntarily relinquish to telephone companies, the use of pen registers by government agents is immune from Fourth Amendment scrutiny. Since I remain convinced that constitutional protections are not abrogated whenever a person apprises another of facts valuable in criminal investigations, see, e. g., *United States v. White*, 401 U. S. 745, 786–790 (1971) (Harlan, J., dissenting); *id.*, at 795–796 (MARSHALL, J., dissenting); *California Bankers Assn. v. Shultz*, 416 U. S. 21, 95–96 (1974) (MARSHALL, J., dissenting); *United States v. Miller*, 425 U. S. 435, 455–456 (1976) (MARSHALL, J., dissenting), I respectfully dissent.

Applying the standards set forth in *Katz v. United States*, 389 U. S. 347, 361 (1967) (Harlan, J., concurring), the Court first determines that telephone subscribers have no subjective expectations of privacy concerning the numbers they dial. To reach this conclusion, the Court posits that individuals somehow infer from the long-distance listings on their phone bills, and from the cryptic assurances of “help” in tracing obscene

calls included in "most" phone books, that pen registers are regularly used for recording local calls. See *ante*, at 742-743. But even assuming, as I do not, that individuals "typically know" that a phone company monitors calls for internal reasons, *ante*, at 743,¹ it does not follow that they expect this information to be made available to the public in general or the government in particular. Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes. See *California Bankers Assn. v. Shultz*, *supra*, at 95-96 (MARSHALL, J., dissenting).

The crux of the Court's holding, however, is that whatever expectation of privacy petitioner may in fact have entertained regarding his calls, it is not one "society is prepared to recognize as 'reasonable.'" *Ante*, at 743. In so ruling, the Court determines that individuals who convey information to third parties have "assumed the risk" of disclosure to the government. *Ante*, at 744, 745. This analysis is misconceived in two critical respects.

Implicit in the concept of assumption of risk is some notion of choice. At least in the third-party consensual surveillance cases, which first incorporated risk analysis into Fourth Amendment doctrine, the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications. See, e. g., *Lopez v. United States*, 373 U. S. 427, 439 (1963); *Hoffa v. United States*, 385 U. S. 293, 302-303 (1966); *United States v. White*, *supra*, at 751-752

¹ Lacking the Court's apparently exhaustive knowledge of this Nation's telephone books and the reading habits of telephone subscribers, see *ante*, at 742-743, I decline to assume general public awareness of how obscene phone calls are traced. Nor am I persuaded that the scope of Fourth Amendment protection should turn on the concededly "esoteric functions" of pen registers in corporate billing, *ante*, at 742, functions with which subscribers are unlikely to have intimate familiarity.

MARSHALL, J., dissenting

442 U.S.

(plurality opinion). By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. Cf. *Lopez v. United States*, *supra*, at 465–466 (BRENNAN, J., dissenting). It is idle to speak of “assuming” risks in contexts where, as a practical matter, individuals have no realistic alternative.

More fundamentally, to make risk analysis dispositive in assessing the reasonableness of privacy expectations would allow the government to define the scope of Fourth Amendment protections. For example, law enforcement officials, simply by announcing their intent to monitor the content of random samples of first-class mail or private phone conversations, could put the public on notice of the risks they would thereafter assume in such communications. See Amsterdam, Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 384, 407 (1974). Yet, although acknowledging this implication of its analysis, the Court is willing to concede only that, in some circumstances, a further “normative inquiry would be proper.” *Ante*, at 740–741, n. 5. No meaningful effort is made to explain what those circumstances might be, or why this case is not among them.

In my view, whether privacy expectations are legitimate within the meaning of *Katz* depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society. By its terms, the constitutional prohibition of unreasonable searches and seizures assigns to the judiciary some prescriptive responsibility. As Mr. Justice Harlan, who formulated the standard the Court applies today, himself recognized: “[s]ince it is the task of the law to form and project, as well as mirror and reflect, we should not . . . merely recite . . . risks without examining the desirability of saddling them upon society.” *United States v. White*, *supra*, at 786 (dissenting opinion). In making this

assessment, courts must evaluate the "intrinsic character" of investigative practices with reference to the basic values underlying the Fourth Amendment. *California Bankers Assn. v. Shultz*, 416 U. S., at 95 (MARSHALL, J., dissenting). And for those "extensive intrusions that significantly jeopardize [individuals'] sense of security . . . , more than self-restraint by law enforcement officials is required." *United States v. White*, 401 U. S., at 786 (Harlan, J., dissenting).

The use of pen registers, I believe, constitutes such an extensive intrusion. To hold otherwise ignores the vital role telephonic communication plays in our personal and professional relationships, see *Katz v. United States*, 389 U. S., at 352, as well as the First and Fourth Amendment interests implicated by unfettered official surveillance. Privacy in placing calls is of value not only to those engaged in criminal activity. The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts. See *NAACP v. Alabama*, 357 U. S. 449, 463 (1958); *Branzburg v. Hayes*, 408 U. S. 665, 695 (1972); *id.*, at 728-734 (STEWART, J., dissenting). Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society. Particularly given the Government's previous reliance on warrantless telephonic surveillance to trace reporters' sources and monitor protected political activity,² I am unwilling to insulate use of pen registers from independent judicial review.

² See, e. g., *Reporters Committee For Freedom of Press v. American Tel. & Tel. Co.*, 192 U. S. App. D. C. 376, 593 F. 2d 1030 (1978), cert. denied, 440 U. S. 949 (1979); *Halperin v. Kissinger*, 434 F. Supp. 1193 (DC 1977); *Socialist Workers Party v. Attorney General*, 463 F. Supp. 515 (SDNY 1978).

MARSHALL, J., dissenting

442 U.S.

Just as one who enters a public telephone booth is "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world," *Katz v. United States*, *supra*, at 352, so too, he should be entitled to assume that the numbers he dials in the privacy of his home will be recorded, if at all, solely for the phone company's business purposes. Accordingly, I would require law enforcement officials to obtain a warrant before they enlist telephone companies to secure information otherwise beyond the government's reach.

**U.S. Copyright Law
(title 17 of U.S. code)
governs the reproduction
and redistribution of
copyrighted material.**

**Downloading this
document for the
purpose of
redistribution is
prohibited.**

ASPEN PUBLISHERS

PRIVACY, INFORMATION, AND TECHNOLOGY

Second Edition

Daniel J. Solove

Professor of Law

George Washington University Law School

Paul M. Schwartz

Professor of Law

U.C. Berkeley Law School



Wolters Kluwer
Law & Business

AUSTIN BOSTON CHICAGO NEW YORK THE NETHERLANDS

© 2009 Aspen Publishers. All Rights Reserved.
<http://lawschool.aspenpublishers.com>

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the publisher. Requests for permission to make copies of any part of this publication should be mailed to:

Aspen Publishers
Attn: Permissions Department
76 Ninth Avenue, 7th Floor
New York, NY 10011-5201

To contact Customer Care, e-mail customer.care@aspenpublishers.com, call 1-800-234-1660, fax 1-800-901-9075, or mail correspondence to:

Aspen Publishers
Attn: Order Department
PO Box 990
Frederick, MD 21705

Printed in the United States of America.

1 2 3 4 5 6 7 8 9 0

ISBN 978-0-7355-7910-1

Library of Congress Cataloging-in-Publication Data

Solove, Daniel J., 1972-

Privacy, information, and technology / Daniel J. Solove, Paul M. Schwartz. — 2nd ed.
p. cm.

ISBN 978-0-7355-7910-1

1. Privacy, Right of — United States. 2. Data protection — Law and legislation — United States. I. Schwartz, Paul M., 1959-. II. Title.

KF1262.S664 2008
342.7308'58 — dc22

2008044313

created a new sunset of December 31, 2009 for USA PATRIOT Act sections 205 and 215 (which concern “roving” FISA wiretaps and FISA orders for business records), and for FISA’s “lone wolf” amendments. This law also expanded the list of predicate offenses for which law enforcement could obtain wiretap orders.

C. DIGITAL SEARCHES AND SEIZURES

1. SEARCHING THE CONTENTS OF COMPUTERS

The Scope of Warrants to Search Computers. In *United States v. Lacy*, 119 F.3d 742 (9th Cir. 1997), the defendant challenged a search warrant authorizing the seizure of his computer hard drive and disks. The defendant contended that the warrant was too general because it applied to his entire computer system. The court upheld the warrant because “this type of generic classification is acceptable when a more precise description is not possible.” Several other courts have followed a similar approach as in *Lacy*, upholding generic warrants. In *United States v. Upham*, 168 F.3d 532 (1st Cir. 1999), the court reasoned: “A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs.” See also *United States v. Hay*, 231 F.3d 630 (9th Cir. 2000) (following *Lacy* and upholding a “generic” warrant application).⁵⁸

However, there are limits to the scope of a search of a computer. In *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), an officer obtained a warrant to search a computer for records about illegal drug distribution. When the officer stumbled upon a pornographic file, he began to search for similar files. The court concluded that these actions amounted to an expansion of the scope of the search and would require the obtaining of a second warrant.

In *United States v. Campos*, 221 F.3d 1143 (10th Cir. 2000), the defendant emailed two images of child pornography to a person he talked to in a chat room. The person informed the FBI, and the FBI obtained a warrant to search the defendant’s home and computer. The agents seized the defendant’s computer, and a search revealed the two images of child pornography as well as six other images of child pornography. The defendant challenged the search as beyond the scope of the warrant because the agents “had grounds to search only for the two images that had been sent.” However, the court rejected the defendant’s contention, quoting from the FBI’s explanation why it is not feasible to search only for particular computer files in one’s home:

. . . Computer storage devices . . . can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is

⁵⁸ For more about computer searches, see Raphael Winnick, *Searches and Seizures of Computers and Computer Data*, 88 Harv. J.L. & Tech. 75 (1994).

included in the warrant. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site. . . .

Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The wide variety of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. . . . Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code embedded into the system as “booby trap”), the controlled environment of a laboratory is essential to its complete analysis. . . .

Computer Searches and Seizures. Searches and seizures for digital information in computers present some unique conceptual puzzles for existing Fourth Amendment doctrine. Thomas Clancy contends:

[C]omputers are containers. . . . They . . . contain electronic evidence, that is, a series of digitally stored 0s and 1s that, when combined with a computer program, yield such items as images, words, and spreadsheets. Accordingly, the traditional standards of the Fourth Amendment regulate obtaining the evidence in containers that happen to be computers.⁵⁹

But is a computer a single container or is each computer file its own container? Orin Kerr argues:

A single physical storage device can store the private files of thousands of different users. It would be quite odd if looking at one file on a server meant that the entire server had been searched, and that the police could then analyze everything on the server, perhaps belonging to thousands of different people, without any restriction.⁶⁰

Is copying a computer file or other digital information a seizure under the Fourth Amendment? In *United States v. Gorshkov*, 2001 WL 1024026 (W.D. Wash. 2001), the FBI remotely copied the contents of the defendant’s computer in Russia. The court held: “The agents’ act of copying the data on the Russian computers was not a seizure under the Fourth Amendment because it did not interfere with Defendant’s or anyone else’s possessory interest in the data.” However, as Susan Brenner and Barbara Frederiksen contend:

[T]he information contained in computer files clearly belongs to the owner of the files. The ownership of information is similar to the contents of a private conversation in which the information belongs to the parties to the conversation. Copying computer data is analogous to recording a conversation. . . . Therefore, copying computer files should be treated as a seizure.⁶¹

⁵⁹ Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 Miss. L.J. 193, 196 (2005).

⁶⁰ Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 556 (2005).

⁶¹ Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 Mich. Telecomm. & Tech. L. Rev. 39, 111-12 (2002).

Password-Protected Files. In *Trulock v. Freeh*, 275 F.3d 391 (4th Cir. 2001), Notra Trulock and Linda Conrad shared a computer but maintained separate files protected by passwords. They did not know each other's password and could not access each other's files. When FBI officials, without a warrant, asked to search and seize the computer, Conrad consented. The court held that the FBI could not search Trulock's files since Trulock had not consented:

Consent to search in the absence of a warrant may, in some circumstances, be given by a person other than the target of the search. Two criteria must be met in order for third party consent to be effective. First, the third party must have authority to consent to the search. Second, the third party's consent must be voluntary....

We conclude that, based on the facts in the complaint, Conrad lacked authority to consent to the search of Trulock's files. Conrad and Trulock both used a computer located in Conrad's bedroom and each had joint access to the hard drive. Conrad and Trulock, however, protected their personal files with passwords; Conrad did not have access to Trulock's passwords. Although Conrad had authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files.

UNITED STATES V. ANDRUS

483 F.3d 711 (10th Cir. 2007)

[Federal authorities believed that Ray Andrus was downloading child pornography to his home computer. Ray Andrus resided at his parents' house. Federal officials obtained the consent of Dr. Andrus (Andrus's father) to search the home. He also consented to their searching any computers in the home. The officials went into Ray Andrus's bedroom and a forensic expert examined the contents of the computer's hard drive with forensic software. The software enabled direct access to the computer, bypassing any password protection the user put on it. The officials discovered child pornography on the computer. Later on, the officials learned that Ray Andrus had protected his computer with a password and that his father did not know the password. Is the father's consent to search the computer valid since he did not know the password?]

MURPHY, J. . . . Subject to limited exceptions, the Fourth Amendment prohibits warrantless searches of an individual's home or possessions. Voluntary consent to a police search, given by the individual under investigation or by a third party with authority over the subject property, is a well-established exception to the warrant requirement. Valid third party consent can arise either through the third party's actual authority or the third party's apparent authority. A third party has actual authority to consent to a search "if that third party has either (1) mutual use of the property by virtue of joint access, or (2) control for most purposes." Even where actual authority is lacking, however, a third party has apparent authority to consent to a search when an officer reasonably, even if erroneously, believes the third party possesses authority to consent. See *Georgia v. Randolph*, 547 U.S. 103 (2006).

Whether apparent authority exists is an objective, totality-of-the-circumstances inquiry into whether the facts available to the officers at the time they commenced the search would lead a reasonable officer to believe the third party had authority to consent to the search. When the property to be searched is an object or container, the relevant inquiry must address the third party's relationship to the object. In *Randolph*, the Court explained, "The constant element in assessing Fourth Amendment reasonableness in consent cases . . . is the great significance given to widely shared social expectations." For example, the Court said, "[W]hen it comes to searching through bureau drawers, there will be instances in which even a person clearly belonging on the premises as an occupant may lack any perceived authority to consent." . . .

It may be unreasonable for law enforcement to believe a third party has authority to consent to the search of an object typically associated with a high expectation of privacy, especially when the officers know or should know the owner has indicated the intent to exclude the third party from using or exerting control over the object.

Courts considering the issue have attempted to analogize computers to other items more commonly seen in Fourth Amendment jurisprudence. Individuals' expectations of privacy in computers have been likened to their expectations of privacy in "a suitcase or briefcase." Password-protected files have been compared to a "locked footlocker inside the bedroom." *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001).

Given the pervasiveness of computers in American homes, this court must reach some, at least tentative, conclusion about the category into which personal computers fall. A personal computer is often a repository for private information the computer's owner does not intend to share with others. . . .

The inquiry into whether the owner of a highly personal object has indicated a subjective expectation of privacy traditionally focuses on whether the subject suitcase, footlocker, or other container is physically locked. Determining whether a computer is "locked," or whether a reasonable officer should know a computer may be locked, presents a challenge distinct from that associated with other types of closed containers. Unlike footlockers or suitcases, where the presence of a locking device is generally apparent by looking at the item, a "lock" on the data within a computer is not apparent from a visual inspection of the outside of the computer, especially when the computer is in the "off" position prior to the search. Data on an entire computer may be protected by a password, with the password functioning as a lock, or there may be multiple users of a computer, each of whom has an individual and personalized password-protected "user profile." . . .

Courts addressing the issue of third party consent in the context of computers, therefore, have examined officers' knowledge about password protection as an indication of whether a computer is "locked" in the way a footlocker would be. For example, in *Trulock*, the Fourth Circuit held a live-in girlfriend lacked actual authority to consent to a search of her boyfriend's computer files where the girlfriend told police she and her boyfriend shared the household computer but had separate password-protected files that were inaccessible to the other. The court in that case explained, "Although Conrad had

authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files." . . .

In addition to password protection, courts also consider the location of the computer within the house and other indicia of household members' access to the computer in assessing third party authority. Third party apparent authority to consent to a search has generally been upheld when the computer is located in a common area of the home that is accessible to other family members under circumstances indicating the other family members were not excluded from using the computer. In contrast, where the third party has affirmatively disclaimed access to or control over the computer or a portion of the computer's files, even when the computer is located in a common area of the house, courts have been unwilling to find third party authority.

Andrus' case presents facts that differ somewhat from those in other cases. Andrus' computer was located in a bedroom occupied by the homeowner's fifty-one year old son rather than in a true common area. Dr. Andrus, however, had unlimited access to the room. Law enforcement officers did not ask specific questions about Dr. Andrus' use of the computer, but Dr. Andrus said nothing indicating the need for such questions. *Cf. Trulock*, 275 F.3d at 398 (when law enforcement questioned third party girlfriend about computer, she indicated she and boyfriend had separate password-protected files). The resolution of this appeal turns on whether the officers' belief in Dr. Andrus' authority was reasonable, despite the lack of any affirmative assertion by Dr. Andrus that he used the computer and despite the existence of a user profile indicating Ray Andrus' intent to exclude other household members from using the computer. For the reasons articulated below, this court concludes the officers' belief in Dr. Andrus' authority was reasonable. . . .

First, the officers knew Dr. Andrus owned the house and lived there with family members. Second, the officers knew Dr. Andrus' house had internet access and that Dr. Andrus paid the Time Warner internet and cable bill. Third, the officers knew the email address bandrus@kc.rr.com had been activated and used to register on a website that provided access to child pornography. Fourth, although the officers knew Ray Andrus lived in the center bedroom, they also knew that Dr. Andrus had access to the room at will. Fifth, the officers saw the computer in plain view on the desk in Andrus' room and it appeared available for use by other household members. Furthermore, the record indicates Dr. Andrus did not say or do anything to indicate his lack of ownership or control over the computer when Cheatham asked for his consent to conduct a computer search. It is uncontested that Dr. Andrus led the officers to the bedroom in which the computer was located, and, even after he saw Kanatzar begin to work on the computer, Dr. Andrus remained silent about any lack of authority he had over the computer. Even if Ray Andrus' computer was protected with a user name and password, there is no indication in the record that the officers knew or had reason to believe such protections were in place.

Andrus argues his computer's password protection indicated his computer was "locked" to third parties, a fact the officers would have known had they asked questions of Dr. Andrus prior to searching the computer. Under our case law, however, officers are not obligated to ask questions unless the circumstances are ambiguous. In essence, by suggesting the onus was on the officers to ask

about password protection prior to searching the computer, despite the absence of any indication that Dr. Andrus' access to the computer was limited by a password, Andrus necessarily submits there is inherent ambiguity whenever police want to search a household computer and a third party has not affirmatively provided information about his own use of the computer or about password protection. Andrus' argument presupposes, however, that password protection of home computers is so common that a reasonable officer ought to know password protection is likely. Andrus has neither made this argument directly nor proffered any evidence to demonstrate a high incidence of password protection among home computer users. . . .

Viewed under the requisite totality-of-the-circumstances analysis, the facts known to the officers at the time the computer search commenced created an objectively reasonable perception that Dr. Andrus was, at least, *one* user of the computer. That objectively reasonable belief would have been enough to give Dr. Andrus apparent authority to consent to a search. Even if Dr. Andrus had no actual ability to use the computer and the computer was password protected, these mistakes of fact do not negate a determination of Dr. Andrus' apparent authority. In this case, the district court found Agent Cheatham properly halted the search when further conversation with Dr. Andrus revealed he did not use the computer and that Andrus' computer was the only computer in the house. These later revelations, however, have no bearing on the reasonableness of the officers' belief in Dr. Andrus' authority at the outset of the computer search.

MCKAY, J., dissenting. This case concerns the reasonable expectation of privacy associated with password-protected computers. In examining the contours of a third party's apparent authority to consent to the search of a home computer, the majority correctly indicates that the extent to which law enforcement knows or should reasonably suspect that password protection is enabled is critical. . . . I take issue with the majority's implicit holding that law enforcement may use software deliberately designed to automatically bypass computer password protection based on third-party consent without the need to make a reasonable inquiry regarding the presence of password protection and the third party's access to that password.

The presence of security on Defendant's computer is undisputed. Yet, the majority curiously argues that Defendant's use of password protection is inconsequential because Defendant failed to argue that computer password protection is "commonplace." Of course, the decision provides no guidance on what would constitute sufficient proof of the prevalence of password protection, nor does it explain why the court could not take judicial notice that password protection is a standard feature of operating systems. Despite recognizing the "pervasiveness of computers in American homes," and the fact that the "personal computer is often a repository for private information the computer's owner does not intend to share with others," the majority requires the invocation of magical language in order to give effect to Defendant's subjective intent to exclude others from accessing the computer. . . .

The unconstrained ability of law enforcement to use forensic software such as the EnCase program to bypass password protection without first determining whether such passwords have been enabled does not "exacerbate[]" this

difficulty; rather, it avoids it altogether, simultaneously and dangerously sidestepping the Fourth Amendment in the process. Indeed, the majority concedes that if such protection were “shown to be commonplace, law enforcement’s use of forensic software like EnCase . . . may well be subject to question.” But the fact that a computer password “lock” may not be *immediately* visible does not render it unlocked. I appreciate that unlike the locked file cabinet, computers have no handle to pull. But, like the padlocked footlocker, computers do exhibit outward signs of password protection: they display boot password screens, username/password log-in screens, and/or screen-saver reactivation passwords.

The fact remains that EnCase’s ability to bypass security measures is well known to law enforcement. Here, ICE’s forensic computer specialist found Defendant’s computer turned off. Without turning it on, he hooked his laptop directly to the hard drive of Defendant’s computer and ran the EnCase program. The agents made no effort to ascertain whether such security was enabled prior to initiating the search. . . .

The majority points out that law enforcement “did not ask specific questions” about Dr. Andrus’ use of the computer or knowledge of Ray Andrus’ use of password protection, but twice criticizes Dr. Andrus’ failure to affirmatively disclaim ownership of, control over, or knowledge regarding the computer. Of course, the computer was located in Ray Andrus’ very tiny bedroom, but the majority makes no effort to explain how this does not create an ambiguous situation as to ownership.

The burden on law enforcement to identify ownership of the computer was minimal. A simple question or two would have sufficed. Prior to the computer search, the agents questioned Dr. Andrus about Ray Andrus’ status as a renter and Dr. Andrus’ ability to enter his 51-year-old son’s bedroom in order to determine Dr. Andrus’ ability to consent to a search of the room, but the agents did not inquire whether Dr. Andrus used the computer, and if so, whether he had access to his son’s password. At the suppression hearing, the agents testified that they were not immediately aware that Defendant’s computer was the only one in the house, and they began to doubt Dr. Andrus’ authority to consent when they learned this fact. The record reveals that, upon questioning, Dr. Andrus indicated that there was a computer in the house and led the agents to Defendant’s room. The forensic specialist was then summoned. It took him approximately fifteen to twenty minutes to set up his equipment, yet, bizarrely, at no point during this period did the agents inquire about the presence of any other computers. . . .

Accordingly, in my view, given the case law indicating the importance of computer password protection, the common knowledge about the prevalence of password usage, and the design of EnCase or similar password bypass mechanisms, the Fourth Amendment and the reasonable inquiry rule, mandate that in consent-based, warrantless computer searches, law enforcement personnel inquire or otherwise check for the presence of password protection and, if a password is present, inquire about the consenter’s knowledge of that password and joint access to the computer. . . .

NOTES & QUESTIONS

1. A Question of Perspective? Orin Kerr contends:

From a virtual user's perspective, the child pornography was hidden to the father; it was behind a password-protected gate. Under these facts, the father couldn't consent to a search because he would lack common authority over it. From a physical perspective, however, the file was present on the hard drive just like all the other information. Under these facts, the father could consent to the search because he had access rights to the machine generally. . . .

Viewed from the physical perspective, the investigators reasonably did not know about the user profile and reasonably believed that the father had rights to consent to that part of the hard drive.⁶²

2. Checking for Password Protection. Was the investigators' belief about the father's authority over the computer reasonable? Should the investigators have asked the father more questions about his use of the computer first? Should they have turned on the machine to see if it was password-protected before hooking up the forensic software? What kinds of incentives does this decision engender for officers doing an investigation?

2. ENCRYPTION

Encryption includes the ability to keep communications secure by concealing the contents of a message. With encryption, even if a communication is intercepted, it still remains secure. Encryption works by translating a message into a code of letters or numbers called "cypher text." The parties to the communication hold a *key*, which consists of the information necessary to translate the code back to the original message, or "plain text." Since ancient times, code-makers have devised cryptographic systems to encode messages. But along with the code-makers arose code-breakers, who were able to figure out the keys to cryptographic systems by, for example, examining the patterns in the encoded messages and comparing them to patterns in a particular language and the frequency of use of certain letters in that language. Today, computers have vastly increased the complexity of encryption.

Encryption presents a difficult trade-off between privacy and surveillance. It is an essential technique to protect the privacy of electronic communications in an age when such communications can so easily be intercepted and monitored. On the other hand, it enables individuals to disguise their communications from detection by law enforcement officials.⁶³ As Whitfield Diffie and Susan Landau observe:

⁶² Orin Kerr, *Virtual Analogies, Physical Searches, and the Fourth Amendment*, Volokh Conspiracy, Apr. 26, 2007, <http://www.volokh.com/posts/1177562355.shtml>.

⁶³ For more background on encryption, see Simon Singh, *The Code: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography* (1999); Steven Levy, *Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age* (2002); A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. Pa. L. Rev. 709 (1995); Robert C. Post, *Encryption Source Code and the First Amendment*, 15 Berkeley Tech. L.J. 713 (2000); A. Michael Froomkin, *The Constitution and Encryption Regulation: Do We Need a "New Privacy"?*, 3 N.Y.U. J. Legis. & Pub. Pol'y 25 (1999).

The explosion in cryptography and the US government's attempts to control it have given rise to a debate between those who hail the new technology's contribution to privacy, business, and security and those who fear both its interference with the work of police and its adverse effect on the collection of intelligence. Positions have often been extreme. The advocates for unfettered cryptography maintain that a free society depends on privacy to protect freedom of association, artistic creativity, and political discussion. The advocates of control hold that there will be no freedom at all unless we can protect ourselves from criminals, terrorists, and foreign threats. Many have tried to present themselves as seeking to maintain or restore the status quo. For the police, the status quo is the continued ability to wiretap. For civil libertarians, it is the ready availability of conversational privacy that prevailed at the time of the country's founding.⁶⁴

The Clipper Chip. The U.S. government has become increasingly concerned that the growing sophistication of encryption would make it virtually impossible for the government to decrypt. In 1994, the government proposed implementing the "Clipper Chip," a federal encryption standard in which the government would retain a copy of the key in a system called "key escrow." By holding a "spare key," the government could readily decrypt encrypted communications if it desired. The Clipper Chip was strongly criticized, and the government's encryption standard has not been widely used.

Encryption and the First Amendment. In *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000), the Sixth Circuit concluded that encryption was protected speech under the First Amendment:

Much like a mathematical or scientific formula, one can describe the function and design of encryption software by a prose explanation; however, for individuals fluent in a computer programming language, source code is the most efficient and precise means by which to communicate ideas about cryptography.

Junger relied on the reasoning of *Bernstein v. United States Dep't of Justice*, 176 F.3d 1132 (9th Cir. 1999) (opinion withdrawn), where the Ninth Circuit struck down a licensing scheme on encryption source code as a violation of the First Amendment:

Bernstein has submitted numerous declarations from cryptographers and computer programmers explaining that cryptographic ideas and algorithms are conveniently expressed in source code. . . . [T]he chief task for cryptographers is the development of secure methods of encryption. While the articulation of such a system in layman's English or in general mathematical terms may be useful, the devil is, at least for cryptographers, often in the algorithmic details. By utilizing source code, a cryptographer can express algorithmic ideas with precision and methodological rigor that is otherwise difficult to achieve. . . .

Thus, cryptographers use source code to express their scientific ideas in much the same way that mathematicians use equations or economists use graphs. . . .

⁶⁴ Whitfield Diffie & Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (1998).

In light of these considerations, we conclude that encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes. . . .

Orin Kerr takes issue with *Junger*'s holding: "the court viewed source code using the close-up paradigm of what the code looked like, rather than the deeper functional perspective of what the code was actually supposed to do. . . . Just as viewing a Seurat painting from inches away reveals only dots, the *Junger* court's myopic view of source code revealed only communications that looked like speech in form, but lacked the deeper significance required to establish constitutional expression."⁶⁵

Consider *Karn v. United States Dep't of State*, 925 F. Supp. 1 (D.D.C. 1996), where the court came to the contrary conclusion from *Junger*:

. . . The government regulation at issue here is clearly content-neutral. . . . The defendants are not regulating the export of the diskette because of the expressive content of the comments and or source code, but instead are regulating because of the belief that the combination of encryption source code on machine readable media will make it easier for foreign intelligence sources to encode their communications. . . .

. . . [A] content-neutral regulation is justified . . . if it is within the constitutional power of the government, it "furthers an important or substantial governmental interest," and "the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." . . .

. . . By placing cryptographic products on the ITAR, the President has determined that the proliferation of cryptographic products will harm the United States. . . .

. . . [T]he plaintiff has not advanced any argument that the regulation is "substantially broader than necessary" to prevent the proliferation of cryptographic products. Nor has the plaintiff articulated any present barrier to the spreading of information on cryptography "by any other means" other than those containing encryption source code on machine-readable media. Therefore, the Court holds that the regulation of the plaintiff's diskette is narrowly tailored to the goal of limiting the proliferation of cryptographic products and that the regulation is justified. . . .

Encryption and the Fourth Amendment. Suppose law enforcement officials legally obtain an encrypted communication. Does the Fourth Amendment require a warrant before the government can decrypt an encrypted communication? Consider the following argument by Orin Kerr:

Encryption is often explained as a lock-and-key system, in which a "key" is used to "lock" plaintext by turning it into ciphertext, and then a "key" is used to "unlock" the ciphertext by turning it into plaintext. We know that locking a container is a common way to create a reasonable expectation of privacy in its contents: the government ordinarily cannot break the lock and search a closed container without a warrant. . . .

⁶⁵ Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 Wash. & Lee L. Rev. 1287, 1292-93 (2000).

When we use a “lock” and “unlock” in the metaphorical sense to denote understanding, however, a lock cannot trigger the rights-based Fourth Amendment. If I tell you a riddle, I do not have a right to stop you from figuring it out. Although figuring out the secret of an inscrutable communication may “unlock” its meaning, the Fourth Amendment cannot regulate such a cognitive discovery. . . .⁶⁶

Encryption and the Fifth Amendment. Can the government compel the production of a private key if it is stored on a personal computer? What if the key is known only to the individual and not stored or recorded?

3. E-MAIL

STEVE JACKSON GAMES, INC. V. UNITED STATES SECRET SERVICE

36 F.3d 457 (5th Cir. 1994)

BARKSDALE, J. Appellant Steve Jackson Games, Incorporated (SJG), publishes books, magazines, role-playing games, and related products. Starting in the mid-1980s, SJG operated an electronic bulletin board system, called “Illuminati” (BBS), from one of its computers. SJG used the BBS to post public information about its business, games, publications, and the role-playing hobby; to facilitate play-testing of games being developed; and to communicate with its customers and free-lance writers by electronic mail (E-mail).

Central to the issue before us, the BBS also offered customers the ability to send and receive private E-mail. Private E-mail was stored on the BBS computer’s hard disk drive temporarily, until the addressees “called” the BBS (using their computers and modems) and read their mail. After reading their E-mail, the recipients could choose to either store it on the BBS computer’s hard drive or delete it. In February 1990, there were 365 BBS users. Among other uses, appellants Steve Jackson, Elizabeth McCoy, William Milliken, and Steffan O’Sullivan used the BBS for communication by private E-mail. . . . [In addition, Lloyd Blankenship, an employee of Steve Jackson Games, operated a computer bulletin bulletin board system (BBS).] Blankenship had the ability to review, and perhaps delete any data on the BBS.

On February 28, 1990, [Secret Service] Agent Foley applied for a warrant to search SJG’s premises and Blankenship’s residence for evidence of violations of 18 U.S.C. §§ 1030 (proscribes interstate transportation of computer access information) and 2314 (proscribes interstate transportation of stolen property). A search warrant for SJG was issued that same day, authorizing the seizure of [computer hardware, software, and computer data.]

The next day, March 1, the warrant was executed by the Secret Service, including Agents Foley and Golden. Among the items seized was the computer which operated the BBS. At the time of the seizure, 162 items of unread, private

⁶⁶ Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a Reasonable Expectation of Privacy?*, 33 Conn. L. Rev. 503, 520-21, 522 (2001).

E-mail were stored on the BBS, including items addressed to the individual appellants. . . .

Appellants filed suit in May 1991 against, among others, the Secret Service and the United States, claiming [among other things, a violation of] the Federal Wiretap Act, as amended by Title I of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2521; and Title II of the ECPA, 18 U.S.C. §§ 2701-2711. . . .

As stated, the sole issue is a very narrow one: whether the seizure of a computer on which is stored private E-mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, constitutes an “intercept” proscribed by 18 U.S.C. § 2511(1)(a).

Section 2511 was enacted in 1968 as part of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, often referred to as the Federal Wiretap Act. Prior to the 1986 amendment by Title I of the ECPA, it covered only wire and oral communications. Title I of the ECPA extended that coverage to electronic communications. In relevant part, § 2511(1)(a) proscribes “intentionally intercept[ing] . . . any wire, oral, or electronic communication,” unless the intercept is authorized by court order or by other exceptions not relevant here. Section 2520 authorizes, *inter alia*, persons whose electronic communications are intercepted in violation of § 2511 to bring a civil action against the interceptor for actual damages, or for statutory damages of \$10,000 per violation or \$100 per day of the violation, whichever is greater. 18 U.S.C. § 2520.

The Act defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4). . . .

Webster’s Third New International Dictionary (1986) defines “aural” as “of or relating to the ear” or “of or relating to the sense of hearing.” And, the Act defines “aural transfer” as “a transfer containing the human voice at any point between and including the point of origin and the point of reception.” 18 U.S.C. § 2510(18). This definition is extremely important for purposes of understanding the definition of a “wire communication,” which is defined by the Act as

any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) . . . and such term includes any electronic storage of such communication.

18 U.S.C. § 2510(1) (emphasis added). In contrast, as noted, an “electronic communication” is defined as “any *transfer* of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . but does not include . . . any wire or oral communication. . . .” 18 U.S.C. § 2510(12) (emphasis added).

Critical to the issue before us is the fact that, unlike the definition of “wire communication,” the definition of “electronic communication” does not include electronic storage of such communications. See 18 U.S.C. § 2510(12). “Electronic storage” is defined as

- (A) any *temporary*, intermediate *storage* of a wire or *electronic communication incidental to the electronic transmission thereof*; and
- (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. . . .

18 U.S.C. § 2510(17) (emphasis added). The E-mail in issue was in “electronic storage.” Congress’ use of the word “transfer” in the definition of “electronic communication,” and its omission in that definition of the phrase “any electronic storage of such communication” (part of the definition of “wire communication”) reflects that Congress did not intend for “intercept” to apply to “electronic communications” when those communications are in “electronic storage.” . . .

Title II generally proscribes unauthorized access to stored wire or electronic communications. Section 2701(a) provides:

Except as provided in subsection (c) of this section whoever —

- (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
- (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication *while it is in electronic storage in such system* shall be punished. . . .

18 U.S.C. § 2701(a) (emphasis added).

As stated, the district court found that the Secret Service violated § 2701 when it

intentionally accessed[d] without authorization a facility [the computer] through which an electronic communication service [the BBS] is provided . . . and thereby obtain[ed] [and] prevent[ed] authorized access [by appellants] to a[n] . . . electronic communication while it is in electronic storage in such system.

18 U.S.C. § 2701(a). The Secret Service does not challenge this ruling. We find no indication in either the Act or its legislative history that Congress intended for conduct that is clearly prohibited by Title II to furnish the basis for a civil remedy under Title I as well. . . .

NOTES & QUESTIONS

1. ***Interception vs. Electronic Storage.*** Is unread e-mail in storage because it is sitting on a hard drive at the ISP? Or is it in transmission because the recipient hasn’t read it yet? Is the court applying an overly formalistic and strict reading of “interception”?
2. ***The Fourth Amendment and E-mail: A Question of Perspective?*** Suppose the police sought to obtain a person’s unread e-mail messages that were stored with her ISP waiting to be downloaded. *Steve Jackson Games* demonstrates how ECPA would apply — the weaker provisions of the Stored Communications Act rather than the stronger protections of the Wiretap Act apply to e-mail temporarily stored with a person’s ISP. *Steve Jackson Games* is a civil case. In the criminal law context, the Stored Communications Act requires a warrant to obtain e-mails stored at the ISP for 180 days or less. If the e-mails

have been stored over 180 days, then the government can obtain them with a mere subpoena.

Would the Fourth Amendment apply? Orin Kerr argues that the answer depends upon the perspective by which one views the Internet. In the “internal perspective,” the Internet is viewed as a virtual world, analogous to real space. From the “external perspective,” we view the Internet as a network and do not analogize to real space. Kerr provides the following example:

Does the Fourth Amendment require [the police] to obtain a search warrant [to obtain an e-mail]? . . . The answer depends largely upon whether they apply an internal or external perspective of the Internet.

Imagine that the first officer applies an internal perspective of the Internet. To him, e-mail is the cyberspace equivalent of old-fashioned postal mail. His computer announces, “You’ve got mail!” when an e-mail message arrives and shows him a closed envelope. When he clicks on the envelope, it opens, revealing the message. From his internal perspective, the officer is likely to conclude that the Fourth Amendment places the same restriction on government access to e-mail that it places on government access to ordinary postal mail. He will then look in a Fourth Amendment treatise for the black letter rule on accessing postal mail. That treatise will tell him that accessing a suspect’s mail ordinarily violates the suspect’s “reasonable expectation of privacy,” and that therefore the officer must first obtain a warrant. Because e-mail is the equivalent of postal mail, the officer will conclude that the Fourth Amendment requires him to obtain a warrant before he can access the e-mail.

Imagine that the second police office approaches the same problem from an external perspective. To him, the facts look quite different. Looking at how the Internet actually works, the second police officer sees that when A sent the e-mail to B, A was instructing his computer to send a message to his Internet Service Provider (ISP) directing the ISP to forward a text message to B’s ISP. To simplify matters, let’s say that A’s ISP is EarthLink, and B’s ISP is America Online (AOL). . . .

What process does the Fourth Amendment require? The second officer will reason that A sent a copy of the e-mail communication to a third party (the EarthLink computer), disclosing the communication to the third party and instructing it to send the communication to yet another third party (AOL). The officer will ask, what process does the Fourth Amendment require to obtain information that has been disclosed to a third party and is in the third party’s possession? The officer will look in a Fourth Amendment treatise and locate to the black letter rule that the Fourth Amendment permits the government to obtain information disclosed to a third party using a mere subpoena. The officer can simply subpoena the system administrator to compel him to produce the e-mails. No search warrant is required.

Who is right? The first officer or the second? The answer depends on whether you approach the Internet from an internal or external perspective. From an internal perspective, the officers need a search warrant; from the external perspective, they do not.⁶⁷

⁶⁷ Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 Geo. L.J. 357, 361-62, 365-67 (2003).

- 3. Previously Read E-mail Stored at an ISP.** The e-mail stored on the ISP server in *Steve Jackson Games* had not yet been downloaded and read by the recipients. Many people continue to store their e-mail messages with their ISP even after having read them. Does the Stored Communications Act protect them in the same way? The answer to this question is currently in dispute. Daniel Solove observes:

Because these messages are now stored indefinitely, according to the DOJ's interpretation . . . the e-mail is no longer in temporary storage and is "simply a remotely stored file." Therefore, under this view, it falls outside of much of the Act's protections. Since many people store their e-mail messages after reading them and the e-mail they send out, this enables the government to access their communications with very minimal limitations.⁶⁸

In *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), the court concluded that

[t]he [Stored Communications] Act defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." Id. § 2510(17), incorporated by id. § 2711(1). Several courts have held that subsection (A) covers e-mail messages stored on an ISP's server pending delivery to the recipient. Because subsection (A) applies only to messages in "temporary, intermediate storage," however, these courts have limited that subsection's coverage to messages not yet delivered to their intended recipient.

Defendants point to these cases and argue that messages remaining on an ISP's server after delivery no longer fall within the Act's coverage. But, even if such messages are not within the purview of subsection (A), they do fit comfortably within subsection (B)

An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again — if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition.

See also Fraser v. Nationwide Mutual Insurance Co., 352 F.3d 108 (3d Cir. 2003) (suggesting that such e-mail messages were in backup storage under the definition of electronic storage).

- 4. What Constitutes an Interception?** In *United States v. Councilman*, 373 F.3d 197 (1st Cir. 2004), an Internet bookseller, Interloc, Inc., provided e-mail service for its customers, who were book dealers. Councilman, the vice president of Interloc, directed Interloc employees to draft a computer program to intercept all incoming communications from Amazon.com to the book dealers and make copies of them. Councilman and other Interloc then read the

⁶⁸ Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 Geo. Wash. L. Rev. 1264 (2004).

e-mails in order to gain a commercial advantage. Councilman was charged with criminal violations of the Wiretap Act. Councilman argued that he did not violate the Wiretap Act because the e-mails were in electronic storage, albeit very briefly, when they were copied. The court followed *Steve Jackson Games* and concluded that the e-mail was in temporary storage and therefore subject to the Stored Communications Act, not the Wiretap Act. However, unlike *Steve Jackson Games*, Interloc accessed the e-mails “as they were being transmitted and in real time.”

The *Councilman* case received significant criticism by academic commentators and experts in electronic surveillance law for misunderstanding the fundamental distinction between the interception of a communication and the accessing of a stored communication. An interception occurs contemporaneously — as the communication is being transmitted. Accessing a stored communication occurs later, as the communication sits on a computer. This distinction has practical consequences, since interceptions are protected by the much more protective Wiretap Act rather than the Stored Communications Act. Does such a distinction still make sense? Is the contemporaneous interception of communications more troublesome than the accessing of the communications in *Steve Jackson Games*?

The case was reheard en banc, and the en banc court reversed the panel. See *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (en banc). The court concluded that “the term ‘electronic communication’ includes transient electronic storage that is intrinsic to the communication process, and hence that interception of an e-mail message in such storage is an offense under the Wiretap Act.” The court declined to further elaborate on what constitutes and “interception.”

5. ***Carnivore*.** Beginning in 1998, the FBI began using a hardware and software mechanism called “Carnivore” to intercept people’s e-mail and instant messaging information from their Internet Service Providers (ISPs). After obtaining judicial authorization, the FBI would install Carnivore by connecting a computer directly to the ISP’s server and initiating the program. Carnivore was designed to locate the e-mails of a suspect at the ISP when the ISP did not have the capacity to do so.

Carnivore was capable of analyzing the entire e-mail traffic of an ISP, although the FBI maintained it was only used to search for the e-mails of a suspect. The program filtered out the e-mail messages of ISP subscribers who are not the subject of the investigation; but to do so, it had to scan the e-mail headers that identify the senders and recipients. The FBI likened e-mail headers to the information captured by a pen register, a device that registers the phone numbers a person dials.

However, Carnivore could be programmed to search through the entire text of all e-mails, to capture e-mails with certain key words. In this way, Carnivore resembles a wiretap. Recall that under federal wiretap law, judicial approval for obtaining pen register information only requires a certification that “the information likely to be obtained by such installation and use is relevant to an ongoing investigation.” 18 U.S.C. § 3123. In contrast, judicial

approval of a wiretap requires a full panoply of requirements under Title I, including a showing of probable cause.

To eliminate the negative associations with the term “Carnivore,” the device was renamed “DCS1000.” Many members of Congress viewed Carnivore with great suspicion. Congress held hearings over the summer of 2000 pertaining to Carnivore, and several bills were proposed to halt or limit the use of Carnivore.

The anti-Carnivore sentiment abruptly ended after the September 11, 2001, World Trade Center and Pentagon terrorist attacks. Section 216 of the USA PATRIOT Act of 2001, in anticipation of the use of Carnivore, required reports on the use of Carnivore to be filed with a court. These reports, filed under seal, require (1) the names of the officers using the device; (2) when the device was installed, used, and removed; (3) the configuration of the device; and (4) the information collected by the device. 18 U.S.C. § 3133(a)(3).

The FBI discontinued use of Carnivore because ISPs can readily produce the information the FBI desires without the assistance of the Carnivore device and because commercially available software has similar functionality.

4. ISP RECORDS

UNITED STATES V. HAMBRICK

55 F. Supp. 2d 504 (W.D. Va. 1999)

MICHAEL, J. Defendant Scott M. Hambrick seeks the suppression of all evidence obtained from his Internet Service Provider (“ISP”), MindSpring, and seeks the suppression of all evidence seized from his home pursuant to a warrant issued by this court. For the reasons discussed below, the court denies the defendant’s motion.

On March 14, 1998, J. L. McLaughlin, a police officer with the Keene, New Hampshire Police Department, connected to the Internet and entered a chat room called “Gay dads 4 sex.” McLaughlin’s screen name was “Rory14.” In this chat room, Detective McLaughlin encountered someone using the screen name “Blowuinva.” Based on a series of online conversations between “Rory14” (Det. McLaughlin) and “Blowuinva,” McLaughlin concluded that “Blowuinva” sought to entice a fourteen-year-old boy to leave New Hampshire and live with “Blowuinva.” Because of the anonymity of the Internet, Detective McLaughlin did not know the true identity of the person with whom he was communicating nor did he know where “Blowuinva” lived. “Blowuinva” had only identified himself as “Brad.”

To determine Blowuinva’s identity and location, McLaughlin obtained a New Hampshire state subpoena that he served on Blowuinva’s Internet Service Provider, MindSpring, located in Atlanta, Georgia. The New Hampshire state subpoena requested that MindSpring produce “any records pertaining to the billing and/or user records documenting the subject using your services on March 14th, 1998 at 1210HRS (EST) using Internet Protocol Number 207.69.169.92.” MindSpring complied with the subpoena. On March 20, 1998, MindSpring

supplied McLaughlin with defendant's name, address, credit card number, e-mail address, home and work telephone numbers, fax number, and the fact that the Defendant's account was connected to the Internet at the Internet Protocol (IP) address.

A justice of the peace, Richard R. Richards, signed the New Hampshire state subpoena. Mr. Richards is not only a New Hampshire justice of the peace, but he is also a detective in the Keene Police Department, Investigation Division. Mr. Richards did not issue the subpoena pursuant to a matter pending before himself, any other judicial officer, or a grand jury. At the hearing on the defendant's motion, the government conceded the invalidity of the warrant. The question before this court, therefore, is whether the court must suppress the information obtained from MindSpring, and all that flowed from it, because the government failed to obtain a proper subpoena. . . .

. . . [Under *Katz v. United States*,] the Fourth Amendment applies only where: (1) the citizen has manifested a subjective expectation of privacy, and (2) the expectation is one that society accepts as "objectively reasonable." . . . Applying the first part of the *Katz* analysis, Mr. Hambrick asserts that he had a subjective expectation of privacy in the information that MindSpring gave to the government. However, resolution of this matter hinges on whether Mr. Hambrick's expectation is one that society accepts as "objectively reasonable."

The objective reasonableness prong of the privacy test is ultimately a value judgment and a determination of how much privacy we should have as a society. In making this constitutional determination, this court must employ a sort of risk analysis, asking whether the individual affected should have expected the material at issue to remain private. The defendant asserts that the Electronic Communications Privacy Act ("ECPA") "legislatively resolves" this question. . . .

The information obtained through the use of the government's invalid subpoena consisted of the defendant's name, address, social security number, credit card number, and certification that the defendant was connected to the Internet on March 14, 1998. Thus, this information falls within the provisions of Title II of the ECPA.

The government may require that an ISP provide stored communications and transactional records only if (1) it obtains a warrant issued under the Federal Rules of Criminal Procedure or state equivalent, or (2) it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of the information in question. See 18 U.S.C. § 2703(a)-(c)(1)(B). When an ISP discloses stored communications or transactional records to a government entity without the requisite authority, the aggrieved customer's sole remedy is damages.

Although Congress is willing to recognize that individuals have some degree of privacy in the stored data and transactional records that their ISPs retain, the ECPA is hardly a legislative determination that this expectation of privacy is one that rises to the level of "reasonably objective" for Fourth Amendment purposes. Despite its concern for privacy, Congress did not provide for suppression where a party obtains stored data or transactional records in violation of the Act. Additionally, the ECPA's concern for privacy extends only to government invasions of privacy. ISPs are free to turn stored data and transactional records over to nongovernmental entities. See 18 U.S.C. § 2703(c)(1)(A) ("[A] provider

of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service . . . to any person other than a governmental entity.”). For Fourth Amendment purposes, this court does not find that the ECPA has legislatively determined that an individual has a reasonable expectation of privacy in his name, address, social security number, credit card number, and proof of Internet connection. The fact that the ECPA does not proscribe turning over such information to private entities buttresses the conclusion that the ECPA does not create a reasonable expectation of privacy in that information. This, however, does not end the court’s inquiry. This court must determine, within the constitutional framework that the Supreme Court has established, whether Mr. Hambrick’s subjective expectation of privacy is one that society is willing to recognize.

To have any interest in privacy, there must be some exclusion of others. To have a reasonable expectation of privacy under the Supreme Court’s risk-analysis approach to the Fourth Amendment, two conditions must be met: (1) the data must not be knowingly exposed to others, and (2) the Internet service provider’s ability to access the data must not constitute a disclosure. In *Katz*, the Supreme Court expressly held that “what a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection.” Further, the Court “consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). . . .

When Scott Hambrick surfed the Internet using the screen name “Blowuinva,” he was not a completely anonymous actor. It is true that an average member of the public could not easily determine the true identity of “Blowuinva.” Nevertheless, when Mr. Hambrick entered into an agreement to obtain Internet access from MindSpring, he knowingly revealed his name, address, credit card number, and telephone number to MindSpring and its employees. Mr. Hambrick also selected the screen name “Blowuinva.” When the defendant selected his screen name it became tied to his true identity in all MindSpring records. MindSpring employees had ready access to these records in the normal course of MindSpring’s business, for example, in the keeping of its records for billing purposes, and nothing prevented MindSpring from revealing this information to nongovernmental actors.⁶⁹ Also, there is nothing in the record to suggest that there was a restrictive agreement between the defendant and MindSpring that would limit the right of MindSpring to reveal the defendant’s personal information to nongovernmental entities. Where such dissemination of information to nongovernment entities is not prohibited, there can be no reasonable expectation of privacy in that information.

Although not dispositive to the outcome of this motion, it is important to note that the court’s decision does not leave members of cybersociety without privacy protection. Under the ECPA, Internet Service Providers are civilly liable when they reveal subscriber information or the contents of stored communications to

⁶⁹ It is apparently common for ISPs to provide certain information that Mr. Hambrick alleges to be private to marketing firms and other organizations interested in soliciting business from Internet users.

the government without first requiring a warrant, court order, or subpoena. Here, nothing suggests that MindSpring had any knowledge that the facially valid subpoena submitted to it was in fact an invalid subpoena. Had MindSpring revealed the information at issue in this case to the government without first requiring a subpoena, apparently valid on its face, Mr. Hambrick could have sued MindSpring. This is a powerful deterrent protecting privacy in the online world and should not be taken lightly. . . .

NOTES & QUESTIONS

- 1. Is There a Reasonable Expectation of Privacy in ISP Records?** The court in *Hambrick* concludes that there is no reasonable expectation of privacy in ISP records based on the third party doctrine in *Smith v. Maryland*. In *United States v. Kennedy*, 81 F. Supp. 2d 1103 (D. Kan. 2000), the court reached a similar conclusion:

Defendant has not demonstrated an objectively reasonable legitimate expectation of privacy in his subscriber information. . . . “[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Smith v. Maryland*, 442 U.S. 735 (1979). When defendant entered into an agreement with [his ISP], he knowingly revealed all information connected to [his IP address]. He cannot now claim to have a Fourth Amendment privacy interest in his subscriber information.

Is *Smith v. Maryland* controlling on this issue? Is there a way to distinguish *Smith*?

- 2. Statutes as a Basis for a Reasonable Expectation of Privacy?** Hambrick was not seeking relief directly under the Stored Communications Act of ECPA. Why not? Instead, Hambrick asserted he had Fourth Amendment protection in his subscriber records. He argued that under the *Katz* reasonable expectation of privacy test, the ECPA “legislatively resolves” that there is a reasonable expectation of privacy in information that Mindspring gave to the government. Should statutes that protect privacy serve as an indication of a societal recognition of a reasonable expectation of privacy? What are the consequences of using statutes such as ECPA to conclude that the Fourth Amendment applies?
- 3. Is There a Remedy?** Mindspring couldn’t release information to the government without a warrant or subpoena or else it would face civil liability. However, in this case, the government presented Mindspring with a subpoena that Mindspring had no knowledge was invalid. Therefore, it is unlikely that Mindspring would be liable. If the court is correct in its conclusion that 18 U.S.C. § 2703(a)–(c)(1)(B) of the ECPA only applies to the conduct of Internet Service Providers, then is there any remedy against Officer Richards’s blatantly false subpoena? Could a police officer obtain a person’s Internet subscriber information by falsifying a subpoena and escape without any civil liability or exclusionary rule?

5. IP ADDRESSES AND URLs

UNITED STATES V. FORRESTER

512 F.3d 500 (9th Cir. 2008)

FISHER, J. . . . Defendants-appellants Mark Stephen Forrester and Dennis Louis Alba were charged with various offenses relating to the operation of a large Ecstasy-manufacturing laboratory, and were convicted on all counts following a jury trial. They now appeal their convictions and sentences. . . .

During its investigation of Forrester and Alba's Ecstasy-manufacturing operation, the government employed various computer surveillance techniques to monitor Alba's e-mail and Internet activity. The surveillance began in May 2001 after the government applied for and received court permission to install a pen register analogue known as a "mirror port" on Alba's account with PacBell Internet. The mirror port was installed at PacBell's connection facility in San Diego, and enabled the government to learn the to/from addresses of Alba's e-mail messages, the IP addresses of the websites that Alba visited and the total volume of information sent to or from his account. Later, the government obtained a warrant authorizing it to employ imaging and keystroke monitoring techniques, but Alba does not challenge on appeal those techniques' legality or the government's application to use them.

Forrester and Alba were tried by jury. At trial, the government introduced extensive evidence showing that they and their associates built and operated a major Ecstasy laboratory. . . .

Alba contends that the government's surveillance of his e-mail and Internet activity violated the Fourth Amendment and fell outside the scope of the then-applicable federal pen register statute. We hold that the surveillance did not constitute a Fourth Amendment search and thus was not unconstitutional. We also hold that whether or not the computer surveillance was covered by the then-applicable pen register statute — an issue that we do not decide — Alba is not entitled to the suppression of any evidence (let alone the reversal of his convictions) as a consequence.

The Supreme Court held in *Smith v. Maryland* that the use of a pen register (a device that records numbers dialed from a phone line) does not constitute a search for Fourth Amendment purposes. According to the Court, people do not have a subjective expectation of privacy in numbers that they dial because they "realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." Even if there were such a subjective expectation, it would not be one that society is prepared to recognize as reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Therefore the use of a pen register is not a Fourth Amendment search. Importantly, the Court distinguished pen registers from more intrusive

surveillance techniques on the ground that “pen registers do not acquire the *contents* of communications” but rather obtain only the addressing information associated with phone calls.

Neither this nor any other circuit has spoken to the constitutionality of computer surveillance techniques that reveal the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account. We conclude that the surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*. First, e-mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communication. *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users’ imputed knowledge that their calls are completed through telephone company switching equipment. Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. Like telephone numbers, which provide instructions to the “switching equipment that processed those numbers,” e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party’s servers.

Second, e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers. When the government obtains the to/from addresses of a person’s e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses — but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.⁷⁰

⁷⁰ Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators (“URL”) of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person’s Internet activity. For instance, a surveillance technique that captures IP addresses would show only that a person visited the New York Times’ website at <http://www.nytimes.com>, whereas a technique that captures URLs would also divulge the particular articles the person viewed.

The government's surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail. In a line of cases dating back to the nineteenth century, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties. E-mail, like physical mail, has an outside address "visible" to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical. The contents may deserve Fourth Amendment protection, but the address and size of the package do not. . . .

We therefore hold that the computer surveillance techniques that Alba challenges are not Fourth Amendment searches. However, our holding extends only to these particular techniques and does not imply that more intrusive techniques or techniques that reveal more content information are also constitutionally identical to the use of a pen register. . . .

Alba claims that the government's computer surveillance was not only unconstitutional but also beyond the scope of the then-applicable pen register statute, 18 U.S.C. § 3121-27 (amended October 2001). Under both the old and new versions of 18 U.S.C. § 3122, the government must apply for and obtain a court order before it can install and use a pen register. When the surveillance at issue here took place in May-July 2001, the applicable statute defined a pen register as a "device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. § 3127(3). Notwithstanding the government's invocation of this provision and application for and receipt of a court order, Alba maintains that the computer surveillance at issue here did not come within the statutory definition of a "pen register."

Even assuming that Alba is correct in this contention, he would not be entitled to the suppression of the evidence obtained through the computer surveillance. As both the Supreme Court and this court have emphasized, suppression is a disfavored remedy, imposed only where its deterrence benefits outweigh its substantial social costs or (outside the constitutional context) where it is clearly contemplated by the relevant statute. . . . Alba does not point to any statutory language requiring suppression when computer surveillance that is similar but not technically equivalent to a pen register is carried out. Indeed, he does not even identify what law or regulation the government may have violated if its surveillance did not come within the scope of the then-applicable pen register statute. The suppression of evidence under these circumstances is plainly inappropriate.

Our conclusion is bolstered by the fact that suppression still would not be appropriate even if the computer surveillance was covered by the pen register statute. Assuming the surveillance violated the statute, there is no mention of suppression of evidence in the statutory text. Instead, the only penalty specified is that "[w]hoever knowingly violates subsection (a)" by installing or using a pen register without first obtaining a court order "shall be fined under this title or imprisoned not more than one year, or both." 18 U.S.C. § 3121(d).

NOTES & QUESTIONS

- 1. IP Addresses vs. URLs.** The *Forrester* court concludes that e-mail headers and IP addresses are akin to pen registers and that the controlling case is *Smith v. Maryland*. Does *Smith* control because IP address and e-mail header information are not revealing of the contents of the communications or because this information is conveyed to a third party? Recall that in a footnote, the court observes that URLs “might be more constitutionally problematic” because a “URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person’s Internet activity.” However, although IP addresses do not reveal specific parts of a websites that a person visits, they do reveal the various websites that a person visits. Why isn’t this revealing enough to trigger constitutional protections?
- 2. Content vs. Envelope Information.** A key distinction under ECPA, as well as Fourth Amendment law, is between “content” and “envelope” information. Orin Kerr explains the distinction:

... [E]very communications network features two types of information: the contents of communications, and the addressing and routing information that the networks use to deliver the contents of communications. The former is “content information,” and the latter is “envelope information.”

The essential distinction between content and envelope information remains constant across different technologies, from postal mail to email. With postal mail, the content information is the letter itself, stored safely inside its envelope. The envelope information is the information derived from the outside of the envelope, including the mailing and return addresses, the stamp and postmark, and the size and weight of the envelope when sealed.

Similar distinctions exist for telephone conversations. The content information for a telephone call is the actual conversation between participants that can be captured by an audio recording of the call. The envelope information includes the number the caller dials, the number from which the caller dials, the time of the call, and its duration.⁷¹

Under ECPA, content information is generally given strong protection (e.g., the Wiretap Act), whereas envelope information is not (e.g., the Pen Register Act). But is such a distinction viable?

Daniel Solove contends that the distinction breaks down:

When applied to IP addresses and URLs, the envelope/content distinction becomes even more fuzzy. An IP address is a unique number that is assigned to each computer connected to the Internet. Each website, therefore, has an IP address. On the surface, a list of IP addresses is simply a list of numbers; but it is actually much more. With a complete listing of IP addresses, the government can learn quite a lot about a person because it can trace how that person surfs the Internet. The government can learn the names of stores at which a person shops, the political organizations a person finds interesting, a person’s sexual fetishes and fantasies, her health concerns, and so on.

⁷¹ Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn’t*, 97 Nw. U. L. Rev. 607, 611 (2003).

Perhaps even more revealing are URLs. A URL is a pointer — it points to the location of particular information on the Internet. In other words, it indicates where something is located. When we cite to something on the Web, we are citing to its URL. . . . URLs can reveal the specific information that people are viewing on the Web. URLs can also contain search terms. . . .

[Therefore,] the content/envelope distinction is not always clear. In many circumstances, to adapt Marshall McLuhan, the “envelope” is the “content.” Envelope information can reveal a lot about a person’s private activities, sometimes as much (and even more) than can content information.⁷²

Orin Kerr disagrees:

Professor Solove appears to doubt the wisdom of offering lower privacy protection for non-content information. He suggests that the acquisition of non-content information should require a full search warrant based on probable cause. . . .

Despite this, Solove’s suggestion that the law should not offer lesser privacy protection for non-content information is unpersuasive. The main reason is that it is quite rare for non-content information to yield the equivalent of content information. It happens in very particular circumstances, but it remains quite rare, and usually in circumstances that are difficult to predict ex ante. In the Internet context, for example, non-content surveillance typically consists of collecting Internet packets; the packets disclose that a packet was sent from one IP address to another IP address at a particular time. This isn’t very private information, at least in most cases. Indeed, it is usually impossible to know who asked for the packet, or what the packet was about, or what the person who asked for the packet wanted to do, or even if it was a person (as opposed to the computer) who sent for the packet in the first place. Solove focuses on the compelling example of Internet search terms as an example of non-content information that can be the privacy equivalent of content information. This is a misleading example, however, as Internet search terms very well may be contents. . . . Thus, despite the fact that non-content information can yield private information, in the great majority of cases contents of communications implicate privacy concerns on a higher order of magnitude than non-content information, and it makes sense to give greater privacy protections for the former and lesser to the latter.⁷³

Solove replies:

Kerr assumes that a compilation of envelope information is generally less revealing than content information. However, a person may care more about protecting the identities of people with whom she communicates than the content of those communications. Indeed, the identities of the people one communicates with implicates freedom of association under the First Amendment. The difficulty is that the distinction between content and envelope information does not correlate well to the distinction between sensitive and innocuous information. Envelope information can be quite sensitive; content information can be quite innocuous. Admittedly, in many cases, people do not care very much about maintaining privacy over the identities of their friends and

⁷² Solove, *Surveillance Law*, *supra*, at 1287-88.

⁷³ Orin S. Kerr, *A User’s Guide to the Stored Communications Act — and a Legislator’s Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1229 n.142 (2004).

associates. But it is also true that in many cases, the contents of communications are not very revealing as well. Many e-mails are short messages which do not reveal any deep secrets, and even Kerr would agree that this should not lessen their protection under the law. This is because content information has the potential to be quite sensitive — but this is also the case with envelope information.⁷⁴

3. ***The Scope of the Pen Register Act.*** The version of the Pen Register Act in effect when the search took place in *Forrester* was the pre-USA PATRIOT Act version, which defined pen registers more narrowly as “numbers dialed.” The USA PATRIOT Act expanded the definition of pen register to include “dialing, routing, addressing, or signaling information . . . provided, however, that such information shall not include the contents of any communication.” Prior to the USA PATRIOT Act changes, it was an open question as to whether the Pen Register Act applied to e-mail headers, IP addresses, and URLs. The USA PATRIOT Act changes aimed to clarify that the Pen Register Act did apply beyond telephone numbers. E-mail headers seem to fit readily into the new Pen Register Act definition. But what about IP addresses and URLs? They involve “routing” and “addressing” information, but they may also include “the contents” of communications. Do they involve “contents” or are they merely “envelope” information?
4. ***Text Messages.*** In *Quon v. Arch Wireless Operating Co., Ltd.*, 2008 WL 2440559 (9th Cir. 2008), the court held that accessing text messages can constitute a violation of the Stored Communications Act because the messages were stored by the communication service provider as “backup” protection for the user. The court also concluded that the Fourth Amendment protects text message communications because they are “content” information: “We see no meaningful difference between the e-mails at issue in *Forrester* and the text messages at issue here.”
5. ***ECPA and the Exclusionary Rule.*** The *Forrester* court concludes that even if the acquisition of information violated the Pen Register Act, the exclusionary rule is not a remedy under the Act. As discussed earlier in this chapter, many provisions of electronic surveillance law lack an exclusionary rule. In the Wiretap Act, wire and oral communications are protected with an exclusionary rule, but electronic communications are not. Solove argues that “[s]ince e-mail has become a central mode of communication, this discrepancy is baseless.”⁷⁵ Is it? Can you think of a reason why e-mail should receive lesser protection than a phone conversation, which would be protected by the exclusionary rule under the Wiretap Act? Additionally, the Stored Communications Act and Pen Register Act have no exclusionary remedies for any type of communication.

⁷⁴ Solove, *Surveillance Law*, *supra*, at 1288. Susan Freiwald contends that “the current categories of the ECPA do not cover web traffic data. At least one other category of protection is needed. Search terms entered, web-pages visited, and items viewed are neither message contents nor their to/from information.” Freiwald, *Online Surveillance*, *supra*, at 71.

⁷⁵ Solove, *Surveillance Law*, *supra*, at 1282.

Orin Kerr argues the absence of an exclusionary rule in many of ECPA's provisions leads to inadequate judicial attention to ECPA. Without an exclusionary rule, Kerr contends, "criminal defendants have little incentive to raise challenges to the government's Internet surveillance practices." Therefore, many challenges to Internet surveillance practices "tend to be in civil cases between private parties that raise issues far removed from those that animated Congress to pass the statutes." Adding an exclusionary remedy, Kerr argues, would "benefit both civil libertarian and law enforcement interests alike." He writes:

On the civil libertarian side, a suppression remedy would considerably increase judicial scrutiny of the government's Internet surveillance practices in criminal cases. The resulting judicial opinions would clarify the rules that the government must follow, serving the public interest of greater transparency. Less obviously, the change could also benefit law enforcement by altering the type and nature of the disputes over the Internet surveillance laws that courts encounter. Prosecutors would have greater control over the types of cases the courts decided, enjoy more sympathetic facts, and have a better opportunity to explain and defend law enforcement interests before the courts. The statutory law of Internet surveillance would become more like the Fourth Amendment law: a source of vital and enforceable rights that every criminal defendant can invoke, governed by relatively clear standards that by and large respect law enforcement needs and attempt to strike a balance between those needs and privacy interests.⁷⁶

6. ***The Internet vs. the Telephone.*** Susan Freiwald contends that while the 1968 Wiretap Act (Title III) provided powerful and effective protection for telephone communications, ECPA in 1986 did not do the same for online communications:

. . . [O]nline surveillance is even more susceptible to law enforcement abuse and even more threatening to privacy. Therefore, one might expect regulation of online surveillance to be more privacy-protective than traditional wiretapping law. That could not be further from the truth. The law provides dramatically less privacy protection for online activities than for traditional telephone calls and videotapings. Additionally, what makes the Wiretap Act complex makes online surveillance law chaotic. Almost all of the techniques designed to rein in law enforcement have been abandoned in the online context. And, while Congress resolved much of its ambivalence towards wiretapping in 1968, current law suggests the outright hostility of all branches of government to online privacy.⁷⁷

In what ways does federal electronic surveillance law protect Internet communication differently from telephone communication? Should the privacy protections differ in these areas?

⁷⁶ Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 Hastings L.J. 805, 824, 807-08 (2003).

⁷⁷ Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9, 14 (2004).

6. KEY LOGGING DEVICES

UNITED STATES V. SCARFO

180 F. Supp. 2d 572 (D.N.J. 2001)

POLITAN, J. . . . Acting pursuant to federal search warrants, the F.B.I. on January 15, 1999, entered Scarfo and Paolercio's business office, Merchant Services of Essex County, to search for evidence of an illegal gambling and loansharking operation. During their search of Merchant Services, the F.B.I. came across a personal computer and attempted to access its various files. They were unable to gain entry to an encrypted file named "Factors."

Suspecting the "Factors" file contained evidence of an illegal gambling and loansharking operation, the F.B.I. returned to the location and, pursuant to two search warrants, installed what is known as a "Key Logger System" ("KLS") on the computer and/or computer keyboard in order to decipher the passphrase to the encrypted file, thereby gaining entry to the file. The KLS records the keystrokes an individual enters on a personal computer's keyboard. The government utilized the KLS in order to "catch" Scarfo's passphrases to the encrypted file while he was entering them onto his keyboard. Scarfo's personal computer features a modem for communication over telephone lines and he possesses an America Online account. The F.B.I. obtained the passphrase to the "Factors" file and retrieved what is alleged to be incriminating evidence.

On June 21, 2000, a federal grand jury returned a three count indictment against the Defendants charging them with gambling and loansharking. The Defendant Scarfo then filed his motion for discovery and to suppress the evidence recovered from his computer. After oral argument was heard on July 30, 2001, the Court ordered additional briefing by the parties. In an August 7, 2001, Letter Opinion and Order, this Court expressed serious concerns over whether the government violated the wiretap statute in utilizing the KLS on Scarfo's computer. Specifically, the Court expressed concern over whether the KLS may have operated during periods when Scarfo (or any other user of his personal computer) was communicating via modem over telephone lines, thereby unlawfully intercepting wire communications without having applied for a wiretap pursuant to Title III, 18 U.S.C. § 2510.

As a result of these concerns, on August 7, 2001, this Court ordered the United States to file with the Court a report explaining fully how the KLS device functions and describing the KLS technology and how it works vis-à-vis the computer modem, Internet communications, e-mail and all other uses of a computer. In light of the government's grave concern over the national security implications such a revelation might raise, the Court permitted the United States to submit any additional evidence which would provide particular and specific reasons how and why disclosure of the KLS would jeopardize both ongoing and future domestic criminal investigations and national security interests.

The United States responded by filing a request for modification of this Court's August 7, 2001, Letter Opinion and Order so as to comply with the procedures set forth in the Classified Information Procedures Act, Title 18, United States Code, Appendix III, § 1 *et seq.* ("CIPA"). [The FBI contended that

a detailed disclosure of how the KLS worked would negatively affect national security and that this information was classified. After an in camera, ex parte hearing with several officials from the Attorney General's office and the FBI, the court granted the government's request not to release the details of how KLS functioned. Instead, the government would provide Scarfo and his attorneys with an unclassified summary about how KLS worked. Based on that summary, Scarfo contended that the KLS violated the Fourth Amendment because the KLS had the capability of collecting data on all of his keystrokes, not merely those of his passphrase.]

Where a search warrant is obtained, the Fourth Amendment requires a certain modicum of particularity in the language of the warrant with respect to the area and items to be searched and/or seized. The particularity requirement exists so that law enforcement officers are constrained from undertaking a boundless and exploratory rummaging through one's personal property. . . . Because the encrypted file could not be accessed via traditional investigative means, Judge Haneke's Order permitted law enforcement officers to "install and leave behind software, firmware, and/or hardware equipment which will monitor the inputted data entered on Nicodemo S. Scarfo's computer in the TARGET LOCATION so that the F.B.I. can capture the password necessary to decrypt computer files by recording the key related information as they are entered." The Order also allowed the F.B.I. to

search for and seize business records in whatever form they are kept (e.g., written, mechanically or computer maintained and any necessary computer hardware, including computers, computer hard drives, floppy disks or other storage disks or tapes as necessary to access such information, as well as, seizing the mirror hard drive to preserve configuration files, public keys, private keys, and other information that may be of assistance in interpreting the password) — including address and telephone books and electronic storage devices; ledgers and other accounting-type records; banking records and statements; travel records; correspondence; memoranda; notes; calendars; and diaries — that contain information about the identities and whereabouts of conspirators, betting customers and victim debtors, and/or that otherwise reveal the origin, receipt, concealment or distribution of criminal proceeds relating to illegal gambling, loansharking and other racketeering offenses.

On its face, the Order is very comprehensive and lists the items, including the evidence in the encrypted file, to be seized with more than sufficient specificity. *See Andresen v. Maryland*, 427 U.S. 463, 480-81 (1976) (defendant's general warrant claim rejected where search warrant contained, among other things, a lengthy list of specified and particular items to be seized). One would be hard pressed to draft a more specified or detailed search warrant than the May 8, 1999 Order. Indeed, it could not be written with more particularity. It specifically identifies each piece of evidence the F.B.I. sought which would be linked to the particular crimes the F.B.I. had probable cause to believe were committed. Most importantly, Judge Haneke's Order clearly specifies the key piece of the puzzle the F.B.I. sought — Scarfo's passphrase to the encrypted file.

That the KLS certainly recorded keystrokes typed into Scarfo's keyboard *other* than the searched-for passphrase is of no consequence. This does not, as Scarfo argues, convert the limited search for the passphrase into a general

exploratory search. During many lawful searches, police officers may not know the exact nature of the incriminating evidence sought until they stumble upon it. Just like searches for incriminating documents in a closet or filing cabinet, it is true that during a search for a passphrase “some innocuous [items] will be at least cursorily perused in order to determine whether they are among those [items] to be seized.”

Hence, “no tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision.” Where proof of wrongdoing depends upon documents or computer passphrases whose precise nature cannot be known in advance, law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence which is properly specified in the warrant. . . . Accordingly, Scarfo’s claim that the warrants were written and executed as general warrants is rejected. . . .

The principal mystery surrounding this case was whether the KLS intercepted a wire communication in violation of the wiretap statute by recording keystrokes of e-mail or other communications made over a telephone or cable line while the modem operated. These are the only conceivable wire communications which might emanate from Scarfo’s computer and potentially fall under the wiretap statute. . . .

The KLS, which is the exclusive property of the F.B.I., was devised by F.B.I. engineers using previously developed techniques in order to obtain a target’s key and key-related information. As part of the investigation into Scarfo’s computer, the F.B.I. “did not install and operate any component which would search for and record data entering or exiting the computer from the transmission pathway through the modem attached to the computer.” Neither did the F.B.I. “install or operate any KLS component which would search for or record any fixed data stored within the computer.”

Recognizing that Scarfo’s computer had a modem and thus was capable of transmitting electronic communications via the modem, the F.B.I. configured the KLS to avoid intercepting electronic communications typed on the keyboard and simultaneously transmitted in real time via the communication ports. . . . Hence, when the modem was operating, the KLS did not record keystrokes. It was designed to prohibit the capture of keyboard keystrokes whenever the modem operated. Since Scarfo’s computer possessed no other means of communicating with another computer save for the modem, the KLS did not intercept any wire communications. Accordingly, the Defendants’ motion to suppress evidence for violation of Title III is denied. . . .

NOTES & QUESTIONS

1. ***Did the Court Need to Reach the Main Issue?*** Judge Politan discusses the government’s actions in *Scarfo* as if a suppression remedy were available for Scarfo. He finds that a search warrant was not required under the Wiretap Act because of the way in which the FBI’s keylogging device worked; the KLS did not function when the modem was operating. But there was a simpler way to deny Scarfo’s motion: the Wiretap Act does not provide a suppression

remedy for electronic communications. Did Judge Politan assume that a remedy existed according to some theory similar to the *McVeigh* case? Was he simply eager to rule on the KLS issue?

2. ***Recording Thoughts and Ideas.*** Consider the following argument by Raymond Ku:

... By monitoring what an individual enters into her computer as she enters it, the government has the ability to monitor thought itself. Keystroke-recording devices allow the government to record formless thoughts and ideas an individual never intended to share with anyone, never intended to save on the hard drive and never intended to preserve for future reference in any form. The devices also allow the government to record thoughts and ideas the individual may have rejected the moment they were typed. . . .

. . . [T]he techniques used in the *Scarfo* case bring us closer to a world in which the only privacy we are guaranteed is the privacy found in the confines of our own minds.⁷⁸

3. ***Old Technologies in New Bottles?*** A common defense of new technological surveillance devices is that they are analogous to existing technologies. Carnivore can be likened to pen registers; the keystroke monitor in the *Scarfo* case can be analogized to a bug. To what extent are these analogies apt? Are new surveillance technologies, simply old forms of surveillance in new bottles? Or is there something different involved? If so, what is new with these technologies, and how ought they be regulated?
4. ***Magic Lantern.*** The FBI has developed technology through which a keystroke logging device can be installed into a person's computer through a computer virus that is e-mailed to the suspect's computer. The virus keeps track of keystrokes and secretly transmits the information to the government. Thus, the government can install a keystroke logging device without ever having to physically enter one's office or home. Recall your Fourth Amendment analysis of Carnivore. How does Magic Lantern differ with respect to its Fourth Amendment implications? How does your Fourth Amendment analysis of Magic Lantern differ from that of the keystroke logging device in *Scarfo*?

⁷⁸ Raymond Ku, *Think Twice Before You Type*, 163 N.J. L.J. 747 (Feb. 19, 2001).

“I’ve Got Nothing to Hide” and Other Misunderstandings of Privacy

DANIEL J. SOLOVE*

TABLE OF CONTENTS

I.	INTRODUCTION	745
II.	THE “NOTHING TO HIDE” ARGUMENT	748
III.	CONCEPTUALIZING PRIVACY	754
	A. <i>A Pluralistic Conception of Privacy</i>	754
	B. <i>The Social Value of Privacy</i>	760
IV.	THE PROBLEM WITH THE “NOTHING TO HIDE” ARGUMENT.....	764
	A. <i>Understanding the Many Dimensions of Privacy</i>	764
	B. <i>Understanding Structural Problems</i>	768
V.	CONCLUSION	772

I. INTRODUCTION

Since the September 11 attacks, the government has been engaging in extensive surveillance and data mining. Regarding surveillance, in December 2005, the *New York Times* revealed that after September 11, the Bush Administration secretly authorized the National Security Administration (NSA) to engage in warrantless wiretapping of American citizens’ telephone calls.¹ As for data mining, which involves analyzing

* © Daniel J. Solove 2007. Associate Professor, George Washington University Law School; J.D., Yale Law School. Thanks to Chris Hoofnagle, Adam Moore, and Michael Sullivan for helpful comments, and to my research assistant Sheerin Shahinpoor. I develop some of the ideas in this essay in significantly more depth in my forthcoming book, *Understanding Privacy*, to be published by Harvard University Press in May 2008.

1. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts: Secret Order to Widen Domestic Monitoring*, N.Y. TIMES, Dec. 16, 2005, at A1.

personal data for patterns of suspicious behavior, the government has begun numerous programs. In 2002, the media revealed that the Department of Defense was constructing a data mining project, called “Total Information Awareness” (TIA), under the leadership of Admiral John Poindexter.² The vision for TIA was to gather a variety of information about people, including financial, educational, health, and other data. The information would then be analyzed for suspicious behavior patterns. According to Poindexter: “The only way to detect . . . terrorists is to look for patterns of activity that are based on observations from past terrorist attacks as well as estimates about how terrorists will adapt to our measures to avoid detection.”³ When the program came to light, a public outcry erupted, and the U.S. Senate subsequently voted to deny the program funding, ultimately leading to its demise.⁴ Nevertheless, many components of TIA continue on in various government agencies, though in a less systematic and more clandestine fashion.⁵

In May 2006, *USA Today* broke the story that the NSA had obtained customer records from several major phone companies and was analyzing them to identify potential terrorists.⁶ The telephone call database is reported to be the “largest database ever assembled in the world.”⁷ In June 2006, the *New York Times* stated that the U.S. government had been accessing bank records from the Society for Worldwide Interbank Financial Transactions (SWIFT), which handles financial transactions for thousands of banks around the world.⁸ Many people responded with outrage at these announcements, but many others did not perceive much of a problem. The reason for their lack of concern, they explained, was because: “I’ve got nothing to hide.”⁹

The argument that no privacy problem exists if a person has nothing to hide is frequently made in connection with many privacy issues. When the government engages in surveillance, many people believe that there is no threat to privacy unless the government uncovers unlawful activity, in which case a person has no legitimate justification to claim that it

2. John Markoff, *Pentagon Plans a Computer System That Would Peek at Personal Data of Americans*, N.Y. TIMES, Nov. 9, 2002, at A12.

3. John M. Poindexter, *Finding the Face of Terror in Data*, N.Y. TIMES, Sept. 10, 2003, at A25.

4. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 169 (2004).

5. Shane Harris, *TIA Lives On*, NAT’L J., Feb. 25, 2006, at 66.

6. Leslie Cauley, *NSA Has Massive Database of Americans’ Phone Calls*, USA TODAY, May 11, 2006, at A1; Susan Page, *Lawmakers: NSA Database Incomplete*, USA TODAY, June 30, 2006, at A1.

7. Cauley, *supra* note 6, at A1.

8. Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, at A1.

9. See *infra* text accompanying notes 12–33.

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

remain private. Thus, if an individual engages only in legal activity, she has nothing to worry about. When it comes to the government collecting and analyzing personal information, many people contend that a privacy harm exists only if skeletons in the closet are revealed. For example, suppose the government examines one's telephone records and finds out that a person made calls to her parents, a friend in Canada, a video store, and a pizza delivery place. "So what?", that person might say. "I'm not embarrassed or humiliated by this information. If anybody asks me, I'll gladly tell them where I shop. I have nothing to hide."

The "nothing to hide" argument and its variants are quite prevalent in popular discourse about privacy. Data security expert Bruce Schneier calls it the "most common retort against privacy advocates."¹⁰ Legal scholar Geoffrey Stone refers to it as "all-too-common refrain."¹¹ The nothing to hide argument is one of the primary arguments made when balancing privacy against security. In its most compelling form, it is an argument that the privacy interest is generally minimal to trivial, thus making the balance against security concerns a foreordained victory for security. Sometimes the nothing to hide argument is posed as a question: "If you have nothing to hide, then what do you have to fear?" Others ask: "If you aren't doing anything wrong, then what do you have to hide?"

In this essay, I will explore the nothing to hide argument and its variants in more depth. Grappling with the nothing to hide argument is important, because the argument reflects the sentiments of a wide percentage of the population. In popular discourse, the nothing to hide argument's superficial incantations can readily be refuted. But when the argument is made in its strongest form, it is far more formidable.

In order to respond to the nothing to hide argument, it is imperative that we have a theory about what privacy is and why it is valuable. At its core, the nothing to hide argument emerges from a conception of privacy and its value. What exactly is "privacy"? How valuable is privacy and how do we assess its value? How do we weigh privacy against countervailing values? These questions have long plagued those seeking to develop a theory of privacy and justifications for its legal protection.

10. Bruce Schneier, Commentary, *The Eternal Value of Privacy*, WIRED, May 18, 2006, <http://www.wired.com/news/columns/1,70886-0.html>.

11. Geoffrey R. Stone, Commentary, *Freedom and Public Responsibility*, CHI TRIB., May 21, 2006, at 11.

This essay begins in Part II by discussing the nothing to hide argument. First, I introduce the argument as it often exists in popular discourse and examine frequent ways of responding to the argument. Second, I present the argument in what I believe to be its strongest form. In Part III, I briefly discuss my work thus far on conceptualizing privacy. I explain why existing theories of privacy have been unsatisfactory, have led to confusion, and have impeded the development of effective legal and policy responses to privacy problems. In Part IV, I argue that the nothing to hide argument—even in its strongest form—stems from certain faulty assumptions about privacy and its value. The problem, in short, is not with finding an answer to the question: “If you’ve got nothing to hide, then what do you have to fear?” The problem is in the very question itself.

II. THE “NOTHING TO HIDE” ARGUMENT

When discussing whether government surveillance and data mining pose a threat to privacy, many people respond that they have nothing to hide. This argument permeates the popular discourse about privacy and security issues. In Britain, for example, the government has installed millions of public surveillance cameras in cities and towns, which are watched by officials via closed circuit television.¹² In a campaign slogan for the program, the government declares: “If you’ve got nothing to hide, you’ve got nothing to fear.”¹³ In the United States, one anonymous individual from the Department of Justice comments: “If [government officials] need to read my e-mails . . . so be it. I have nothing to hide. Do you?”¹⁴ One blogger, in reference to profiling people for national security purposes, declares: “Go ahead and profile me, I have nothing to hide.”¹⁵ Another blogger proclaims: “So I don’t mind people wanting to find out things about me, I’ve got nothing to hide! Which is why I support President Bush’s efforts to find terrorists by monitoring our phone calls!”¹⁶ Variations of nothing to hide arguments frequently appear in blogs, letters to the editor, television news interviews, and other forums. Some examples include:

12. JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE (2004).

13. *Id.* at 36.

14. Comment of NonCryBaby to <http://www.securityfocus.com/comments/articles/2296/18105/threaded> (Feb. 12, 2003).

15. Comment of Yoven to <http://www.danielpipes.org/comments/47675> (June 14, 2006, 14:03 EST).

16. Reach For The Stars!, <http://greatcarrieoakey.blogspot.com/2006/05/look-all-you-want-ive-got-nothing-to.html> (May 14, 2006, 09:04 PST).

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"
SAN DIEGO LAW REVIEW

- I don't have anything to hide from the government. I don't think I had that much hidden from the government in the first place. I don't think they care if I talk about my ornery neighbor.¹⁷
- Do I care if the FBI monitors my phone calls? I have nothing to hide. Neither does 99.99 percent of the population. If the wiretapping stops one of these Sept. 11 incidents, thousands of lives are saved.¹⁸
- Like I said, I have nothing to hide. The majority of the American people have nothing to hide. And those that have something to hide should be found out, and get what they have coming to them.¹⁹

The argument is not only of recent vintage. For example, one of the characters in Henry James's 1888 novel, *The Reverberator*, muses: "[I]f these people had done bad things they ought to be ashamed of themselves and he couldn't pity them, and if they hadn't done them there was no need of making such a rumpus about other people knowing."²⁰

I encountered the nothing to hide argument so frequently in news interviews, discussions, and the like, that I decided to blog about the issue. I asked the readers of my blog, *Concurring Opinions*, whether there are good responses to the nothing to hide argument.²¹ I received a torrent of comments to my post:

- My response is "So do you have curtains?" or "Can I see your credit card bills for the last year?"²²
- So my response to the "If you have nothing to hide . . ." argument is simply, "I don't need to justify my position. You need to justify yours. Come back with a warrant."²³

17. Comment of annegb to Concurring Opinions, http://www.concurringopinions.com/archives/2006/05/is_there_a_good.html#comments (May 23, 2006, 11:37 EST).

18. Joe Schneider, Letter to the Editor, *NSA Wiretaps Necessary*, ST. PAUL PIONEER PRESS, Aug. 24, 2006, at 11B.

19. *Polls Suggest Americans Approve NSA Monitoring* (NPR radio broadcast, May 19, 2006), available at 2006 WLNR 22949347.

20. HENRY JAMES, THE REVERBERATOR (1888), reprinted in NOVELS 1886–1880, at 555, 687 (1989).

21. Concurring Opinions, *supra* note 17 (May 23, 2006, 00:06 EST).

22. Comment of Adam to Concurring Opinions, *supra* note 17 (May 23, 2006, 16:27 EST).

23. Comment of Dissent to Concurring Opinions, *supra* note 17 (May 24, 2006, 07:48 EST).

- I don't have anything to hide. But I don't have anything I feel like showing you, either.²⁴
- If you have nothing to hide, then you don't have a life.²⁵
- Show me yours and I'll show you mine.²⁶
- It's not about having anything to hide, it's about things not being anyone else's business.
- Bottom line, Joe Stalin would [have] loved it. Why should anyone have to say more?²⁸

Most replies to the nothing to hide argument quickly respond with a witty retort. Indeed, on the surface it seems easy to dismiss the nothing to hide argument. Everybody probably has something to hide from somebody. As the author Aleksandr Solzhenitsyn declared, ‘Everyone is guilty of something or has something to conceal. All one has to do is look hard enough to find what it is.’²⁹ Likewise, in Friedrich Dürrenmatt’s novella *Traps*, which involves a seemingly innocent man put on trial by a group of retired lawyers for a mock trial game, the man inquires what his crime shall be. ‘‘An altogether minor matter,’’ the prosecutor replied ‘A crime can always be found.’³⁰ One can usually think of something compelling that even the most open person would want to hide. As one comment to my blog post noted: ‘If you have nothing to hide, then that quite literally means you are willing to let me photograph you naked? And I get full rights to that photograph—so I can show it to your neighbors?’³¹ Canadian privacy expert David Flaherty expresses a similar idea when he argues:

24. Comment of Ian to Concurring Opinions, *supra* note 17 (May 24, 2006, 19:51 EST).

25. Comment of Matthew Graybosch to Concurring Opinions, *supra* note 17 (Oct. 16, 2006, 12:09 EST).

26. Comment of Neureaux to Concurring Opinions, *supra* note 17 (Oct. 16, 2006, 14:39 EST).

27. Comment of Catter to Concurring Opinions, *supra* note 17 (Oct. 16, 2006, 11:36 PM EST).

28. Comment of Kevin to Concurring Opinions, *supra* note 17 (July 24, 2006, 12:36 EST).

29. ALEKSANDR SOLZHENITSYN, CANCER WARD 192 (Nicholas Bethell & David Burg trans., Noonday Press 1991) (1968).

30. FRIEDRICH DÜRRENMATT, TRAPS 23 (Richard & Clara Winston trans., 1960).

31. Comment of Andrew to Concurring Opinions, *supra* note 17 (Oct. 16, 2006, 15:06 EST).

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"
SAN DIEGO LAW REVIEW

There is no sentient human being in the Western world who has little or no regard for his or her personal privacy; those who would attempt such claims cannot withstand even a few minutes' questioning about intimate aspects of their lives without capitulating to the intrusiveness of certain subject matters.³²

Such responses only attack the nothing to hide argument in its most extreme form, which is not particularly strong. As merely a one-line utterance about a particular person's preference, the nothing to hide argument is not very compelling. But stated in a more sophisticated manner, the argument is more challenging. First, it must be broadened beyond the particular person making it. When phrased as an individual preference, the nothing to hide argument is hard to refute because it is difficult to quarrel with one particular person's preferences. As one commenter aptly notes:

By saying "I have nothing to hide," you are saying that it's OK for the government to infringe on the rights of potentially millions of your fellow Americans, possibly ruining their lives in the process. To me, the "I have nothing to hide" argument basically equates to "I don't care what happens, so long as it doesn't happen to me."³³

In its more compelling variants, the nothing to hide argument can be made in a more general manner. Instead of contending that "I've got nothing to hide," the argument can be recast as positing that all law-abiding citizens should have nothing to hide. Only if people desire to conceal unlawful activity should they be concerned, but according to the nothing to hide argument, people engaged in illegal conduct have no legitimate claim to maintaining the privacy of such activities.

In a related argument, Judge Richard Posner contends: "[W]hen people today decry lack of privacy, what they want, I think, is mainly something quite different from seclusion: they want more power to conceal information about themselves that others might use to their disadvantage."³⁴ Privacy involves a person's "right to conceal discreditable facts about himself."³⁵ In other words, privacy is likely to be invoked when there is something to hide and that something consists of negative

32. David H. Flaherty, *Visions of Privacy: Past, Present, and Future*, in VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 19, 31 (Colin J. Bennett & Rebecca Grant eds., 1999).

33. Comment of BJ Horn to Concurring Opinions, *supra* note 17 (June 2, 2006, 18:58 EST).

34. RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 271 (1983).

35. RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 46 (5th ed. 1998).

information about a person. Posner asserts that the law should not protect people in concealing discreditable information. "The economist," he argues, "sees a parallel to the efforts of sellers to conceal defects in their products."³⁶

Of course, one might object, there is nondiscreditable information about people that they nevertheless want to conceal because they find it embarrassing or just do not want others to know about. In a less extreme form, the nothing to hide argument does not refer to all personal information, but only to that subset of personal information that is likely to be involved in government surveillance. When people respond to NSA surveillance and data mining that they have nothing to hide, the more sophisticated way of understanding their argument should be as applying to the particular pieces of information that are gathered in the NSA programs. Information about what phone numbers people dial and even what they say in many conversations is often not likely to be embarrassing or discreditable to a law-abiding citizen. Retorts to the nothing to hide argument about exposing people's naked bodies to the world or revealing their deepest secrets to their friends are only relevant if there is a likelihood that such programs will actually result in these kinds of disclosures. This type of information is not likely to be captured in the government surveillance. Even if it were, many people might rationally assume that the information will be exposed only to a few law enforcement officials, and perhaps not even seen by human eyes. Computers might store the data and analyze it for patterns, but no person might have any contact with the data. As Posner argues:

The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy. But machine collection and processing of data cannot, as such, invade privacy. Because of their volume, the data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value. This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer.³⁷

There is one final component of the most compelling versions of the nothing to hide argument—a comparison of the relative value of the privacy interest being threatened with the government interest in promoting security. As one commenter to my blog post astutely notes: "You can't talk about how people feel about the potential loss of privacy in any meaningful way without recognizing that most of the people who don't mind the NSA programs see it as a potential exchange of a small

36. *Id.*

37. Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, at A31.

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"
SAN DIEGO LAW REVIEW

amount of privacy for a potential national security gain.³⁸ In other words, the nothing to hide argument can be made by comparing the relative value between privacy and security. The value of privacy, the argument provides, is low, because the information is often not particularly sensitive. The ones with the most to worry about are the ones engaged in illegal conduct, and the value of protecting their privacy is low to nonexistent. On the government interest side of the balance, security has a very high value. Having a computer analyze the phone numbers one dials is not likely to expose deep dark secrets or embarrassing information to the world. The machine will simply move on, oblivious to any patterns that are not deemed suspicious. In other words, if you are not doing anything wrong, you have nothing to hide and nothing to fear.

Therefore, in a more compelling form than is often expressed in popular discourse, the nothing to hide argument proceeds as follows: The NSA surveillance, data mining, or other government information-gathering programs will result in the disclosure of particular pieces of information to a few government officials, or perhaps only to government computers. This very limited disclosure of the particular information involved is not likely to be threatening to the privacy of law-abiding citizens. Only those who are engaged in illegal activities have a reason to hide this information. Although there may be some cases in which the information might be sensitive or embarrassing to law-abiding citizens, the limited disclosure lessens the threat to privacy. Moreover, the security interest in detecting, investigating, and preventing terrorist attacks is very high and outweighs whatever minimal or moderate privacy interests law-abiding citizens may have in these particular pieces of information.

Cast in this manner, the nothing to hide argument is a formidable one. It balances the degree to which an individual's privacy is compromised by the limited disclosure of certain information against potent national security interests. Under such a balancing scheme, it is quite difficult for privacy to prevail.

38. Comment of MJ to Concurring Opinions, *supra* note 17 (May 23, 2006, 17:30 EST).

IV. THE PROBLEM WITH THE “NOTHING TO HIDE” ARGUMENT

A. *Understanding the Many Dimensions of Privacy*

It is time to return to the nothing to hide argument. The reasoning of this argument is that when it comes to government surveillance or use of personal data, there is no privacy violation if a person has nothing sensitive, embarrassing, or illegal to conceal. Criminals involved in illicit activities have something to fear, but for the vast majority of people, their activities are not illegal or embarrassing.

Understanding privacy as I have set forth reveals the flaw of the nothing to hide argument at its roots. Many commentators who respond to the argument attempt a direct refutation by trying to point to things that people would want to hide. But the problem with the nothing to hide argument is the underlying assumption that privacy is about hiding bad things. Agreeing with this assumption concedes far too much ground and leads to an unproductive discussion of information people would likely want or not want to hide. As Bruce Schneier aptly notes, the nothing to hide argument stems from a faulty “premise that privacy is about hiding a wrong.”⁷⁵

The deeper problem with the nothing to hide argument is that it myopically views privacy as a form of concealment or secrecy. But understanding privacy as a plurality of related problems demonstrates that concealment of bad things is just one among many problems caused by government programs such as the NSA surveillance and data mining. In the categories in my taxonomy, several problems are implicated.

The NSA programs involve problems of information collection, specifically the category of surveillance in the taxonomy. Wiretapping involves audio surveillance of people’s conversations. Data mining often begins with the collection of personal information, usually from various third parties that possess people’s data. Under current Supreme Court Fourth Amendment jurisprudence, when the government gathers data from third parties, there is no Fourth Amendment protection because people lack a “reasonable expectation of privacy” in information exposed to others.⁷⁶ In *United States v. Miller*, the Supreme Court concluded that there is no reasonable expectation of privacy in bank records because “[a]ll of the documents obtained, including financial statements and

75. Schneier, *supra* note 10.

76. *United States v. Katz*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"
SAN DIEGO LAW REVIEW

deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.”⁷⁷ In *Smith v. Maryland*, the Supreme Court held that people lack a reasonable expectation of privacy in the phone numbers they dial because they “know that they must convey numerical information to the phone company,” and therefore they cannot “harbor any general expectation that the numbers they dial will remain secret.”⁷⁸ As I have argued extensively elsewhere, the lack of Fourth Amendment protection of third party records results in the government’s ability to access an extensive amount of personal information with minimal limitation or oversight.⁷⁹

Many scholars have referred to information collection as a form of surveillance. *Dataveillance*, a term coined by Roger Clarke, refers to the “systemic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons.”⁸⁰ Christopher Slobogin has referred to the gathering of personal information in business records as “transaction surveillance.”⁸¹ Surveillance can create chilling effects on free speech, free association, and other First Amendment rights essential for democracy.⁸² Even surveillance of legal activities can inhibit people from engaging in them. The value of protecting against chilling effects is not measured simply by focusing on the particular individuals who are deterred from exercising their rights. Chilling effects harm society because, among other things, they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity.

The nothing to hide argument focuses primarily on the information collection problems associated with the NSA programs. It contends that limited surveillance of lawful activity will not chill behavior sufficiently to outweigh the security benefits. One can certainly quarrel with this

77. 425 U.S. 435, 442 (1976).

78. 442 U.S. 735, 743 (1979).

79. SOLOVE, *supra* note 4, at 165–209; see also Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1117–37 (2002).

80. Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. OF THE ACM 498, 499 (1988); see also Roger Clarke, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, AUSTRALIAN NATIONAL UNIVERSITY, Aug. 7, 2006, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.

81. Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 140 (2005).

82. Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 154–59 (2007).

argument, but one of the difficulties with chilling effects is that it is often very hard to demonstrate concrete evidence of deterred behavior.⁸³ Whether the NSA's surveillance and collection of telephone records has deterred people from communicating particular ideas would be a difficult question to answer.

Far too often, discussions of the NSA surveillance and data mining define the problem solely in terms of surveillance. To return to my discussion of metaphor, the problems are not just Orwellian, but Kafkaesque. The NSA programs are problematic even if no information people want to hide is uncovered. In *The Trial*, the problem is not inhibited behavior, but rather a suffocating powerlessness and vulnerability created by the court system's use of personal data and its exclusion of the protagonist from having any knowledge or participation in the process. The harms consist of those created by bureaucracies—indifference, errors, abuses, frustration, and lack of transparency and accountability. One such harm, for example, which I call *aggregation*, emerges from the combination of small bits of seemingly innocuous data.⁸⁴ When combined, the information becomes much more telling about a person. For the person who truly has nothing to hide, aggregation is not much of a problem. But in the stronger, less absolutist form of the nothing to hide argument, people argue that certain pieces of information are not something they would hide. Aggregation, however, means that by combining pieces of information we might not care to conceal, the government can glean information about us that we might really want to conceal. Part of the allure of data mining for the government is its ability to reveal a lot about our personalities and activities by sophisticated means of analyzing data. Therefore, without greater transparency in data mining, it is hard to claim that programs like the NSA data mining program will not reveal information people might want to hide, as we do not know precisely what is revealed. Moreover, data mining aims to be predictive of behavior, striving to prognosticate about our future actions. People who match certain profiles are deemed likely to engage in a similar pattern of behavior. It is quite difficult to refute actions that one has not yet done. Having nothing to hide will not always dispel predictions of future activity.

Another problem in the taxonomy, which is implicated by the NSA program, is the problem I refer to as *exclusion*.⁸⁵ Exclusion is the problem caused when people are prevented from having knowledge about how their information is being used, as well as barred from being

83. *Id.*

84. Solove, *supra* note 56, at 506–11.

85. *Id.* at 522–25.

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"
SAN DIEGO LAW REVIEW

able to access and correct errors in that data. The NSA program involves a massive database of information that individuals cannot access. Indeed, the very existence of the program was kept secret for years.⁸⁶ This kind of information processing, which forbids people's knowledge or involvement, resembles in some ways a kind of due process problem. It is a structural problem involving the way people are treated by government institutions. Moreover, it creates a power imbalance between individuals and the government. To what extent should the Executive Branch and an agency such as the NSA, which is relatively insulated from the political process and public accountability, have a significant power over citizens? This issue is not about whether the information gathered is something people want to hide, but rather about the power and the structure of government.

A related problem involves "secondary use." Secondary use is the use of data obtained for one purpose for a different unrelated purpose without the person's consent. The Administration has said little about how long the data will be stored, how it will be used, and what it could be used for in the future. The potential future uses of any piece of personal information are vast, and without limits or accountability on how that information is used, it is hard for people to assess the dangers of the data being in the government's control.

Therefore, the problem with the nothing to hide argument is that it focuses on just one or two particular kinds of privacy problems—the disclosure of personal information or surveillance—and not others. It assumes a particular view about what privacy entails, and it sets the terms for debate in a manner that is often unproductive.

It is important to distinguish here between two ways of justifying a program such as the NSA surveillance and data mining program. The first way is to not recognize a problem. This is how the nothing to hide argument works—it denies even the existence of a problem. The second manner of justifying such a program is to acknowledge the problems but contend that the benefits of the NSA program outweigh the privacy harms. The first justification influences the second, because the low value given to privacy is based upon a narrow view of the problem.

The key misunderstanding is that the nothing to hide argument views privacy in a particular way—as a form of secrecy, as the right to hide

86. Risen & Lichtblau, *supra* note 1.

things. But there are many other types of harm involved beyond exposing one's secrets to the government.

Privacy problems are often difficult to recognize and redress because they create a panoply of types of harm. Courts, legislators, and others look for particular types of harm to the exclusion of others, and their narrow focus blinds them to seeing other kinds of harms.

B. Understanding Structural Problems

One of the difficulties with the nothing to hide argument is that it looks for a visceral kind of injury as opposed to a structural one. Ironically, this underlying conception of injury is shared by both those advocating for greater privacy protections and those arguing in favor of the conflicting interests to privacy. For example, law professor Ann Bartow argues that I have failed to describe privacy harms in a compelling manner in my article, *A Taxonomy of Privacy*, where I provide a framework for understanding the manifold different privacy problems.⁸⁷ Bartow's primary complaint is that my taxonomy "frames privacy harms in dry, analytical terms that fail to sufficiently identify and animate the compelling ways that privacy violations can negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease."⁸⁸ Bartow claims that the taxonomy does not have "enough dead bodies" and that privacy's "lack of blood and death, or at least of broken bones and buckets of money, distances privacy harms from other categories of tort law."⁸⁹

Most privacy problems lack dead bodies. Of course, there are exceptional cases such as the murders of Rebecca Shaeffer and Amy Boyer. Rebecca Shaeffer was an actress killed when a stalker obtained her address from a Department of Motor Vehicles record.⁹⁰ This incident prompted Congress to pass the Driver's Privacy Protection Act of 1994.⁹¹ Amy Boyer was murdered by a stalker who obtained her personal information, including her work address and Social Security number, from a database company.⁹² These examples aside, there is not a lot of death and gore in privacy law. If this is the standard to recognize a problem, then few privacy problems will be recognized. Horrific cases

87. Ann Bartow, *A Feeling of Unease About Privacy Law*, 155 U. PA. L. REV. PENNUMBRA 52, 52 (2006), <http://www.pennumbra.com/issues/articles/154-3/Bartow.pdf>.

88. *Id.*

89. *Id.* at 52, 62.

90. SOLOVE, *supra* note 4, at 147.

91. *Id.*

92. Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1005–06 (N.H. 2003).

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

are not typical, and the purpose of my taxonomy is to explain why most privacy problems are still harmful despite this fact.

Bartow's objection is actually very similar to the nothing to hide argument. Those advancing the nothing to hide argument have in mind a particular kind of visceral privacy harm, one where privacy is violated only when something deeply embarrassing or discrediting is revealed. Bartow's quest for horror stories represents a similar desire to find visceral privacy harms. The problem is that not all privacy harms are like this. At the end of the day, privacy is not a horror movie, and demanding more palpable harms will be difficult in many cases. Yet there is still a harm worth addressing, even if it is not sensationalistic.

In many instances, privacy is threatened not by singular egregious acts, but by a slow series of relatively minor acts which gradually begin to add up. In this way, privacy problems resemble certain environmental harms which occur over time through a series of small acts by different actors. Bartow wants to point to a major spill, but gradual pollution by a multitude of different actors often creates worse problems.

The law frequently struggles with recognizing harms that do not result in embarrassment, humiliation, or physical or psychological injury.⁹³ For example, after the September 11 attacks, several airlines gave their passenger records to federal agencies in direct violation of their privacy policies. The federal agencies used the data to study airline security.⁹⁴ A group of passengers sued Northwest Airlines for disclosing their personal information. One of their claims was that Northwest Airlines breached its contract with the passengers. In *Dyer v. Northwest Airlines Corp.*, the court rejected the contract claim because "broad statements of company policy do not generally give rise to contract claims," the passengers never claimed they relied upon the policy or even read it, and they "failed to allege any contractual damages arising out of the alleged breach."⁹⁵ Another court reached a similar conclusion.⁹⁶

Regardless of the merits of the decisions on contract law, the cases represent a difficulty with the legal system in addressing privacy problems.

93. SOLOVE, *supra* note 4, at 93–97, 100–01, 195–208; Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1228 (2003).

94. SOLOVE, *supra* note 4, at 93.

95. 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004).

96. *In re Nw. Airlines Privacy Litig.*, No. 04-126, 2004 WL 1278459 (D. Minn. June 6, 2004).

The disclosure of the passenger records represented a “breach of confidentiality.”⁹⁷ The problems caused by breaches of confidentiality do not merely consist of individual emotional distress; they involve a violation of trust within a relationship. There is a strong social value in ensuring that promises are kept and that trust is maintained in relationships between businesses and their customers. The problem of secondary use is also implicated in this case.⁹⁸ Secondary use involves data collected for one purpose being used for an unrelated purpose without people’s consent. The airlines gave passenger information to the government for an entirely different purpose beyond that for which it was originally gathered. Secondary use problems often do not cause financial, or even psychological, injuries. Instead, the harm is one of power imbalance. In *Dyer*, data was disseminated in a way that ignored airline passengers’ interests in the data despite promises made in the privacy policy. Even if the passengers were unaware of the policy, there is a social value in ensuring that companies adhere to established limits on the way they use personal information. Otherwise, any stated limits become meaningless, and companies have discretion to boundlessly use data. Such a state of affairs can leave nearly all consumers in a powerless position. The harm, then, is less one to particular individuals than it is a structural harm.

A similar problem surfaces in another case, *Smith v. Chase Manhattan Bank*.⁹⁹ A group of plaintiffs sued Chase Manhattan Bank for selling customer information to third parties in violation of its privacy policy, which stated that the information would remain confidential. The court held that even presuming these allegations were true, the plaintiffs could not prove any actual injury:

[T]he “harm” at the heart of this purported class action, is that class members were merely offered products and services which they were free to decline. This does not qualify as actual harm.

The complaint does not allege any single instance where a named plaintiff or any class member suffered any actual harm due to the receipt of an unwanted telephone solicitation or a piece of junk mail.¹⁰⁰

The court’s view of harm, however, did not account for the breach of confidentiality.

When balancing privacy against security, the privacy harms are often characterized in terms of injuries to the individual, and the interest in security is often characterized in a more broad societal way. The security

97. Solove, *supra* note 56, at 526–30.

98. *Id.* at 520–22.

99. 741 N.Y.S.2d 100 (N.Y. App. Div. 2002).

100. *Id.* at 102.

[VOL. 44: 745, 2007]

"I've Got Nothing to Hide"

SAN DIEGO LAW REVIEW

interest in the NSA programs has often been defined improperly. In a Congressional hearing, Attorney General Alberto Gonzales stated:

Our enemy is listening, and I cannot help but wonder if they are not shaking their heads in amazement at the thought that anyone would imperil such a sensitive program by leaking its existence in the first place, and smiling at the prospect that we might now disclose even more or perhaps even unilaterally disarm ourselves of a key tool in the war on terror.¹⁰¹

The balance between privacy and security is often cast in terms of whether a particular government information collection activity should or should not be barred.

The issue, however, often is not whether the NSA or other government agencies should be allowed to engage in particular forms of information gathering; rather, it is what kinds of oversight and accountability we want in place when the government engages in searches and seizures. The government can employ nearly any kind of investigatory activity with a warrant supported by probable cause. This is a mechanism of oversight—it forces government officials to justify their suspicions to a neutral judge or magistrate before engaging in the tactic. For example, electronic surveillance law allows for wiretapping, but limits the practice with judicial supervision, procedures to minimize the breadth of the wiretapping, and requirements that the law enforcement officials report back to the court to prevent abuses.¹⁰² It is these procedures that the Bush Administration has ignored by engaging in the warrantless NSA surveillance. The question is not whether we want the government to monitor such conversations, but whether the Executive Branch should adhere to the appropriate oversight procedures that Congress has enacted into law, or should covertly ignore any oversight.

Therefore, the security interest should not get weighed in its totality against the privacy interest. Rather, what should get weighed is the extent of marginal limitation on the effectiveness of a government information gathering or data mining program by imposing judicial oversight and minimization procedures. Only in cases where such procedures will completely impair the government program should the security interest

101. *Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 15 (2006) (statement of Alberto Gonzales, Att'y Gen. of the United States).

102. Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 775–76 (2005).

be weighed in total, rather than in the marginal difference between an unencumbered program versus a limited one.

Far too often, the balancing of privacy interests against security interests takes place in a manner that severely shortchanges the privacy interest while inflating the security interests. Such is the logic of the nothing to hide argument. When the argument is unpacked, and its underlying assumptions examined and challenged, we can see how it shifts the debate to its terms, in which it draws power from its unfair advantage. It is time to pull the curtain on the nothing to hide argument.

V. CONCLUSION

Whether explicit or not, conceptions of privacy underpin nearly every argument made about privacy, even the common quip “I’ve got nothing to hide.” As I have sought to demonstrate in this essay, understanding privacy as a pluralistic conception reveals that we are often talking past each other when discussing privacy issues. By focusing more specifically on the related problems under the rubric of “privacy,” we can better address each problem rather than ignore or conflate them. The nothing to hide argument speaks to some problems, but not to others. It represents a singular and narrow way of conceiving of privacy, and it wins by excluding consideration of the other problems often raised in government surveillance and data mining programs. When engaged with directly, the nothing to hide argument can ensnare, for it forces the debate to focus on its narrow understanding of privacy. But when confronted with the plurality of privacy problems implicated by government data collection and use beyond surveillance and disclosure, the nothing to hide argument, in the end, has nothing to say.

the digital person

Technology and Privacy in the Information Age

daniel j. solove

© 2004 by New York University



NEW YORK UNIVERSITY PRESS *New York and London*

3

Kafka and Orwell

Reconceptualizing Information Privacy

The most widely discussed metaphor in the discourse of information privacy is George Orwell's depiction of Big Brother in *1984*. The use of the Big Brother metaphor to understand the database privacy problem is hardly surprising. Big Brother has long been the metaphor of choice to characterize privacy problems, and it has frequently been invoked when discussing police search tactics,¹ wiretapping and video surveillance,² and drug testing.³ It is no surprise, then, that the burgeoning discourse on information privacy has seized upon this metaphor.

With regard to computer databases, however, Big Brother is incomplete as a way to understand the problem. Although the Big Brother metaphor certainly describes particular facets of the problem, it neglects many crucial dimensions. This oversight is far from inconsequential, for the way we conceptualize a problem has important ramifications for law and policy.

The Importance of Metaphor

A metaphor, as legal scholar Steven Winter aptly defines it, "is the imaginative capacity by which we relate one thing to another."⁴ In

their groundbreaking analysis, linguistics professor George Lakoff and philosopher Mark Johnson observe that metaphors are not mere linguistic embellishments or decorative overlays on experience; they are part of our conceptual systems and affect the way we interpret our experiences? Metaphor is not simply an act of description; it is a way of conceptualization. “The essence of metaphor,” write Lakoff and Johnson, “is understanding and experiencing one kind of thing in terms of another.”⁶

Much of our thinking about a problem involves the metaphors we use. According to legal philosopher Jack Balkin, “metaphoric models selectively describe a situation, and in so doing help to suppress alternative conceptions.” Metaphors do not just distort reality but compose it; the “power [of metaphors] stems precisely from their ability to empower understanding by shaping and hence limiting it.”⁷

Winter, as well as Lakoff and Johnson, focus on metaphors embodied in our thought processes, pervading the type of language we use.⁸ The metaphors I speak of are not as deeply ingrained. Metaphors are tools of shared cultural understanding.⁹ Privacy involves the type of society we are creating, and we often use metaphors to envision different possible worlds, ones that we want to live in and ones that we don’t. Orwell’s Big Brother is an example of this type of metaphor; it is a shared cultural narrative, one that people can readily comprehend and react to.

Ascribing metaphors is not only a descriptive endeavor but also an act of political theorizing with profound normative implications.¹⁰ According to Judge Richard Posner, however, “it is a mistake to try to mine works of literature for political or economic significance” because works of literature are better treated as aesthetic works rather than “as works of moral or political philosophy.”¹¹ To the contrary, literature supplies the metaphors by which we conceptualize certain problems, and Posner fails to acknowledge the role that metaphor plays in shaping our collective understanding. Metaphors function not to render a precise descriptive representation of the problem; rather, they capture our concerns over privacy in a way that is palpable, potent, and compelling. Metaphors are instructive not for their realism but for the way they direct our focus to certain social and political phenomena.

George Orwell's Big Brother

Orwell's Totalitarian World. Journalists, politicians, and jurists often describe the problem created by databases with the metaphor of Big Brother—the harrowing totalitarian government portrayed in George Orwell's *1984*.¹² Big Brother is an all-knowing, constantly vigilant government that regulates every aspect of one's existence. In every corner are posters of an enormous face, with “eyes [that] follow you about when you move” and the caption “BIG BROTHER IS WATCHING YOU.”¹³

Big Brother demands complete obedience from its citizens and controls all aspects of their lives. It constructs the language, rewrites the history, purges its critics, indoctrinates the population, burns books, and obliterates all disagreeable relics from the past. Big Brother's goal is uniformity and complete discipline, and it attempts to police people to an unrelenting degree—even their innermost thoughts. Any trace of individualism is quickly suffocated.

This terrifying totalitarian state achieves its control by targeting the private life, employing various techniques of power to eliminate any sense of privacy. Big Brother views solitude as dangerous. Its techniques of power are predominantly methods of surveillance. Big Brother is constantly monitoring and spying; uniformed patrols linger on street corners; helicopters hover in the skies, poised to peer into windows. The primary surveillance tool is a device called a “telescreen” which is installed into each house and apartment. The telescreen is a bilateral television—individuals can watch it, but it also enables Big Brother to watch them:

There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guess-work. It was even conceivable that they watched everybody all the time.... You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.¹⁴

In *1984*, citizens have no way of discovering if and when they are being watched. This surveillance, both real and threatened, is

combined with swift and terrifying force: “People simply disappeared, always during the night. Your name was removed from the registers, every record of everything you had ever done was wiped out, your one-time existence was denied and then forgotten.”¹⁵

Orwell’s narrative brilliantly captures the horror of the world it depicts, and its images continue to be invoked in the legal discourse of privacy and information. “The ultimate horror in Orwell’s imagined anti-utopia,” observes sociologist Dennis Wrong, “is that men are deprived of the very capacity for cherishing private thoughts and feelings opposed to the regime, let alone acting on them.”¹⁶

Panoptic Power. The telescreen functions similarly to the Panopticon, an architectural design for a prison, originally conceived by Jeremy Bentham in 1791.¹⁷ In *Discipline und Punish*, Michel Foucault provides a Compelling description of this artifice of power:

[A]t the periphery, an annular building; at the centre, a tower; this tower is pierced with wide windows that open onto the inner side of the ring; the peripheric building is divided into cells, each of which extends the whole width of the building. . . . All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy. By the effect of backlighting, one can observe from the tower, standing out precisely against the light, the small captive shadows in the cells of the periphery. They are like so many cages, so many small theatres, in which each actor is alone, perfectly individualized and constantly visible.¹⁸

The Panopticon is a device of discipline; its goal is to ensure order, to prevent plots and riots, to mandate total obedience. The Panopticon achieves its power through an ingenious technique of surveillance, one that is ruthlessly efficient. By setting up a central observation tower from which all prisoners can be observed and by concealing from them any indication of whether they are being watched at any given time, “surveillance is permanent in its effects, even if it is discontinuous in its action.”¹⁹ Instead of having hundreds of patrols and watchpersons, only a few people need to be in the tower. Those in the tower can watch any inmate but they cannot be

seen. By always being visible, by constantly living under the reality that one could be observed at any time, people assimilate the effects of surveillance into themselves. They obey not because they are monitored but because of their fear that they could be watched. This fear alone is sufficient to achieve control. The Panopticon is so efficient that nobody needs to be in the tower at all.

As Foucault observed, the Panopticon is not merely limited to the prison or to a specific architectural structure—it is a technology of power that can be used in many contexts and in a multitude of ways. In 1984, the telescreen works in a similar way to the Panopticon, serving as a form of one-way surveillance that structures the behavior of those who are observed. The collection of information in cyberspace can be readily analogized to the telescreen. As we surf the Internet, information about us is being collected; we are being watched, but we do not know when or to what extent.

The metaphor of Big Brother understands privacy in terms of power, and it views privacy as an essential dimension of the political structure of society. Big Brother attempts to dominate the private life because it is the key to controlling an individual's entire existence: her thoughts, ideas, and actions.

The Ubiquity of the Metaphor. Big Brother dominates the discourse of information privacy. In 1974, when the use of computer databases was in its infancy, U.S. Supreme Court Justice William Douglas observed that we live in an Orwellian age in which the computer has become “the heart of a surveillance system that will turn society into a transparent world.”²⁰ One state supreme court justice observed that the “acres of files” being assembled about us are leading to an “Orwellian society.”²¹

Academics similarly characterize the problem.²² In *The Culture of Surveillance*, sociologist William Staples observes that we have internalized Big Brother—we have created a Big Brother culture, where we all act as agents of surveillance and voyeurism.²³ “The specter of Big Brother has haunted computerization from the beginning,” computer science professor Abbe Mowshowitz observes. “Computerized personal record-keeping systems, in the hands of police and intelligence agencies, clearly extend the surveillance capabilities of the state.”²⁴

Commentators have adapted the Big Brother metaphor to describe the threat to privacy caused by private-sector databases, often referring to businesses as “Little Brothers.”²⁵ As sociologist David Lyon puts it: “Orwell’s dystopic vision was dominated by the central state. He never guessed just how significant a decentralized consumerism might become for social control.”²⁶ Legal scholar Katrin Byford writes: “Life in cyberspace, if left unregulated, thus promises to have distinct Orwellian overtones—with the notable difference that the primary threat to privacy comes not from government, but rather from the corporate world.”²⁷ In *The End of Privacy*, political scientist Reg Whitaker also revises the Big Brother narrative into one of a multitude of Little Brothers.²⁸

Internet “surveillance” can be readily compared to Orwell’s telescreen. While people surf the web, companies are gathering information about them. As Paul Schwartz, a leading expert on privacy law, observes, the “Internet creates digital surveillance with nearly limitless data storage possibilities and efficient search possibilities.” Instead of one Big Brother, today there are a “myriad” of “Big and Little Brothers” collecting personal data.²⁹

Even when not directly invoking the metaphor, commentators frequently speak in its language, evoke its images and symbols, and define privacy problems in similar conceptual terms. Commentators view databases as having many of the same purposes (social control, suppression of individuality) and employing many of the same techniques (surveillance and monitoring) as Big Brother. David Flaherty, who served as the first Information and Privacy Commissioner for British Columbia, explains that the “storage of personal data can be used to limit opportunity and to encourage conformity.” Dossiers of personal information “can have a limiting effect on behavior.”³⁰ Oscar Gandy, a noted professor of communications and media studies, writes that “panopticism serves as a powerful metaphorical resource for representing the contemporary technology of segmentation and targeting.”³¹ As legal scholar Jerry Kang observes:

[D]ata collection in cyberspace produces data that are detailed, computer-processable, indexed to the individual, and perma-

nent. Combine this with the fact that cyberspace makes data collection and analysis exponentially cheaper than in real space, and we have what Roger Clarke has identified as the genuine threat of “**dataveillance**.³²

Dataveillance, as information technology expert Roger Clarke defines it, refers to the “systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons.”³³ According to political scientist Colin Bennet, “[t]he term **dataveillance** has been coined to describe the surveillance practices that the massive collection and storage of vast quantities of personal data have facilitated.”³⁴ Dataveillance is thus a new form of surveillance, a method of watching not through the eye or the camera, but by collecting facts and data. Kang argues that surveillance is an attack on human dignity, interfering with free choice because it “leads to **self-censorship**.³⁵ Likewise, Paul Schwartz claims that data collection “creates a potential for suppressing a capacity for free choice: the more that is known about an individual, the easier it is to force his **obedience**.³⁶ According to this view, the problem with databases is that they are a form of surveillance that curtails individual freedom.

The Limits of the Metaphor. Despite the fact that the discourse appropriately conceptualizes privacy through metaphor and that the Big Brother metaphor has proven quite useful for a number of privacy problems, the metaphor has significant limitations for the database privacy problem. As illustrated by the history of record-keeping and databases in chapter 2, developments in record-keeping were not orchestrated according to a grand scheme but were largely ad hoc, arising as technology interacted with the demands of the growing public and private bureaucracies. Additionally, the goals of data collection have often been rather benign—or at least far less malignant than the aims of Big Brother. In fact, personal information has been collected and recorded for a panoply of purposes. The story of record-keeping and database production is, in the end, not a story about the progression toward a world ruled by Big Brother or a multitude of Little

Brothers. Instead, it is a story about a group of different actors with different purposes attempting to thrive in an increasingly information-based society.

The most significant shortcoming of the Big Brother metaphor is that it fails to focus on the appropriate form of power. The metaphor depicts a particular technique of power—surveillance. Certainly, monitoring is an aspect of information collection, and databases may eventually be used in ways that resemble the disciplinary regime of Big Brother. However, most of the existing practices associated with databases are quite different in character. Direct marketers wish to observe behavior so they can tailor goods and advertisements to individual differences. True, they desire consumers to act in a certain way (to purchase their product), but their limited attempts at control are far from the repressive regime of total control exercised by Big Brother. The goal of much data collection by marketers aims not at suppressing individuality but at studying it and exploiting it.

The most insidious aspect of the surveillance of Big Brother is missing in the context of databases: human judgment about the activities being observed (or the fear of that judgment). Surveillance leads to conformity, inhibition, and self-censorship in situations where it is likely to involve human judgment. Being observed by an insect on the wall is not invasive of privacy; rather, privacy is threatened by being subject to *human* observation, which involves judgments that can affect one's life and reputation. Since marketers generally are interested in aggregate data, they do not care about snooping into particular people's private lives. Much personal information is amassed and processed by computers; we are being watched not by other humans, but by machines, which gather information, compute profiles, and generate lists for mailing, emailing, or calling. This impersonality makes the surveillance less invasive.

While having one's actions monitored by computers does not involve immediate perception by a human consciousness, it still exposes people to the possibility of future review and disclosure. In the context of databases, however, this possibility is remote. Even when such data is used for marketing, marketers merely want to make a profit, not uproot a life or soil a reputation.

I do not, however, want to discount the dangerous effects of surveillance through the use of databases. Although the purposes of the users of personal data are generally not malignant, databases can still result in unintended harmful social effects. The mere knowledge that one's behavior is being monitored and recorded certainly can lead to self-censorship and inhibition. Foucault's analysis of surveillance points to a more subtle yet more pervasive effect: surveillance changes the entire landscape in which people act, leading toward an internalization of social norms that soon is not even perceived as repressive.³⁷ This view of the effects of surveillance raises important questions regarding the amount of normalization that is desirable in society. While our instincts may be to view all normalization as an insidious force, most theories of the good depend upon a significant degree of normalization to hold society together.

Although the effects of surveillance are certainly a part of the database problem, the heavy focus on surveillance **miscomprehends** the most central and pernicious effects of databases. Understanding the problem as surveillance fails to account for the majority of our activities in the world and web. A large portion of our personal information involves facts that we are not embarrassed about: our financial information, race, marital status, hobbies, occupation, and the like. Most people surf the web without wandering into its dark corners. The vast majority of the information collected about us concerns relatively innocuous details. The surveillance model does not explain why the recording of this **non-taboo** information poses a problem. The focus of the surveillance model is on the **fringes**—and often involves things we may indeed want to inhibit such as cult activity, terrorism, and child pornography.

Digital dossiers do cause a serious problem that is overlooked by the Big Brother metaphor, one that poses a threat not just to our freedom to explore the taboo, but to freedom in general. It is a problem that implicates the type of society we are becoming, the way we think, our place in the larger social order, and our ability to exercise meaningful control over our lives.

Franz Kafka's Trial

Kafka's Distopic Vision. Although we cannot arbitrarily adopt new metaphors, we certainly can exercise control over the metaphors we use. Since understanding our current society is an ongoing process, not a once-and-done activity, we are constantly in search of new metaphors to better comprehend our situation.

Franz Kafka's harrowing depiction of bureaucracy in *The Trial* captures dimensions of the digital dossier problem that the Big Brother metaphor does not.³⁸ *The Trial* opens with the protagonist, Joseph K., awakening one morning to find a group of officials in his apartment, who inform him that he is under arrest. K. is bewildered at why he has been placed under arrest: "I cannot recall the slightest offense that might be charged against me. But even that is of minor importance, the real question is, who accuses me? What authority is conducting these proceedings?" When he asks why the officials have come to arrest him, an official replies: "You are under arrest, certainly, more than that I do not know."³⁹ Instead of taking him away to a police station, the officials mysteriously leave.

Throughout the rest of the novel, Joseph K. begins a frustrating quest to discover why he has been arrested and how his case will be resolved. A vast bureaucratic court has apparently scrutinized his life and assembled a dossier on him. The Court is clandestine and mysterious, and court records are "inaccessible to the accused."⁴⁰ In an effort to learn about this Court and the proceedings against him, Joseph K. scuttles throughout the city, encountering a maze of lawyers, priests, and others, each revealing small scraps of knowledge about the workings of the Court. In a pivotal scene, Joseph K. meets a painter who gleaned much knowledge of the obscure workings of the Court while painting judicial portraits. The painter explains to K.:

"The whole dossier continues to circulate, as the regular official routine demands, passing on to the highest Courts, being referred to the lower ones again, and then swinging backwards and forwards with greater or smaller oscillations, longer or shorter delays.... No document is ever lost, the Court never forgets anything. One day—quite unexpectedly—some Judge will take up

the documents and look at them attentively" "And the case begins all over again?" asked K. almost incredulously. "Certainly" said the painter.⁴¹

Ironically, after the initial arrest, it is Joseph K. who takes the initiative in seeking out the Court. He is informed of an interrogation on Sunday, but only if he has no objection to it: "Nevertheless he was hurrying fast, so as if possible to arrive by nine o'clock, although he had not even been required to appear at any specific time."⁴² Although the Court has barely imposed any authority, not even specifying when Joseph K. should arrive for his interrogation, he acts as if this Court operates with strict rules and makes every attempt to obey. After the interrogation, the Court seems to lose interest in him. Joseph K., however, becomes obsessed with his case. He wants to be recognized by the Court and to resolve his case; in fact, being ignored by the Court becomes a worse torment than being arrested.

As K. continues his search, he becomes increasingly perplexed by this unusual Court. The higher officials keep themselves hidden; the lawyers claim they have connections to Court officials but never offer any proof or results. Hardly anyone seems to have direct contact with the Court. In addition, its "proceedings were not only kept secret from the general public, but from the accused as well." Yet K. continues to seek an acquittal from a crime he hasn't been informed of and from an authority he cannot seem to find. As Joseph K. scurries through the bureaucratic labyrinth of the law, he can never make any progress toward his acquittal: "Progress had always been made, but the nature of the progress could never be divulged. The Advocate was always working away at the first plea, but it had never reached a conclusion."⁴³ In the end, Joseph K. is seized by two officials in the middle of the night and executed.

Kafka's *The Trial* best captures the scope, nature, and effects of the type of power relationship created by databases. My point is not that *The Trial* presents a more realistic descriptive account of the database problem than Big Brother. Like *1984*, *The Trial* presents a fictional portrait of a harrowing world, often exaggerating certain elements of society in a way that makes them humorous and absurd. Certainly, in the United States most people are not told that they are inexplicably

under arrest, and they do not expect to be executed unexpectedly one evening. *The Trial* is in part a satire, and what is important for the purposes of my argument are the insights the novel provides about society through its exaggerations. In the context of computer databases, Kafka's *The Trial* is the better focal point for the discourse than Big Brother. Kafka depicts an indifferent bureaucracy, where individuals are pawns, not knowing what is happening, having no say or ability to exercise meaningful control over the process. This lack of control allows the trial to completely take over Joseph K.'s life. *The Trial* captures the sense of helplessness, frustration, and vulnerability one experiences when a large bureaucratic organization has control over a vast dossier of details about one's life. At any time, something could happen to JosephK.; decisions are made based on his data, and JosephK. has no say, no knowledge, and no ability to fight back. He is completely at the mercy of the bureaucratic process.

As understood in light of the Kafka metaphor, the primary problem with databases stems from the way the bureaucratic process treats individuals and their information.

Bureaucracy. Generally, the term “bureaucracy” refers to large public and private organizations with hierarchical structures and a set of elaborate rules, routines, and processes.⁴⁴ I will use the term to refer not to specific institutions but to a particular set of practices—specifically, how bureaucratic processes affect and influence individuals subjected to them. Bureaucratic organization, sociologist Max Weber asserts, consists of a hierarchical chain-of-command, specialized offices to carry out particular functions, and a system of general rules to manage the organization.⁴⁵ Bureaucracy is not limited to government administration; it is also a feature of business management. The modern world requires the efficient flow of information in order to communicate, to deliver goods and services, to regulate, and to carry out basic functions. According to Weber, bureaucracy is “capable of attaining the highest degree of efficiency and is in this sense formally the most rational known means of exercising authority over human beings.”⁴⁶ Bureaucratic processes are highly routinized, striving for increased efficiency, standardization of decisions, and the cultivation of specialization and expertise. As Paul Schwartz notes,

bureaucracy depends upon “vast quantities of information” that “relates to identifiable individuals.”⁴⁷ Much of this information is important and necessary to the smooth functioning of bureaucracies.

Although bureaucratic organization is an essential and beneficial feature of modern society, bureaucracy also presents numerous problems. Weber observes that bureaucracy can become “dehumanized” by striving to eliminate “love, hatred, and all purely personal, irrational, and emotional elements which escape calculation.”⁴⁸ Bureaucracy often cannot adequately attend to the needs of particular individuals—not because bureaucrats are malicious, but because they must act within strict time constraints, have limited training, and are frequently not able to respond to unusual situations in unique or creative ways. Schwartz contends that because bureaucracy does not adequately protect the dignity of the people it deals with, it can “weaken an individual’s capacity for critical reflection and participation in society.”⁴⁹ Additionally, decisions within public and private bureaucratic organizations are often hidden from public view, decreasing accountability. As Weber notes, “[b]ureaucratic administration always tends to exclude the public, to hide its knowledge and action from criticism as well as it can.”⁵⁰ Bureaucratic organizations often have hidden pockets of discretion. At lower levels, discretion can enable abuses. Frequently, bureaucracies fail to train employees adequately and may employ subpar security measures over personal data. Bureaucracies are often careless in their uses and handling of personal information.

The problem with databases emerges from subjecting personal information to the bureaucratic process with little intelligent control or limitation, which results in our not having meaningful participation in decisions about our information. Bureaucratic decision-making processes are being exercised ever more frequently over a greater sphere of our lives, and we have little power or say within such a system, which tends to structure our participation along standardized ways that fail to enable us to achieve our goals, wants, and needs.

Bureaucracy and Power. The power effects of this relationship to bureaucracy are profound; however, they cannot adequately be explained by resorting only to the understanding of power in Orwell’s

1984. Big Brother employs a coercive power that is designed to dominate and oppress. Power, however, is not merely prohibitive; as illustrated by Aldous Huxley in *Brave New World*, it composes our very lives and culture. Huxley describes a different form of totalitarian society—one controlled not by force, but by entertainment and pleasure. The population is addicted to a drug called Soma, which is administered by the government as a political tool to sedate the people. Huxley presents a narrative about a society controlled not by a despotic coercive government like Big Brother, but by manipulation and consumption, where people participate in their own enslavement. The government achieves obedience through social conditioning, propaganda, and other forms of indoctrination.⁵¹ It does not use the crude coercive techniques of violence and force, but instead employs a more subtle scientific method of control—through genetic engineering, psychology, and drugs. Power works internally—the government actively molds the private life of its citizens, transforming it into a world of vapid pleasure, mindlessness, and numbness.

Despite the differences, power for both Orwell and Huxley operates as an insidious force employed for a particular design. *The Trial* depicts a different form of power. The power employed in *The Trial* has no apparent goal; any purpose remains shrouded in mystery. Nor is the power as direct and manipulative in design as that depicted by Orwell and Huxley. The Court system barely even cares about Joseph K. *The Trial* depicts a world that differs significantly from our traditional notions of a totalitarian state. Joseph K. was not arrested for his political views; nor did the Court manifest any plan to control people. Indeed, Joseph K. was searching for some reason why he was arrested, a reason that he never discovered. One frightening implication is that there was no reason, or if there were, it was absurd or arbitrary. Joseph K. was subjected to a more purposeless process than a trial. Indeed, the Court does not try to exercise much power over Joseph K. His arrest does not even involve his being taken into custody—merely a notification that he is under arrest—and after an initial proceeding, the Court makes no further effort even to contact Joseph K.

What is more discernible than any motive on the part of the Court or any overt exercise of power are the social effects of the power relationship between the bureaucracy and Joseph K. The power depicted

in *The Trial* is not so much a force as it is an element of relationships between individuals and society and government. These relationships have balances of power. What *The Trial* illustrates is that power is not merely exercised in totalitarian forms, and that relationships to bureaucracies which are unbalanced in power can have debilitating effects upon individuals—regardless of the bureaucracies' purposes (which may, in fact, turn out to be quite benign).

Under this view, the problem with databases and the practices currently associated with them is that they **disempower** people. They make people vulnerable by stripping them of control over their personal information. There is no diabolical motive or secret plan for domination; rather, there is a web of thoughtless decisions made by low-level bureaucrats, standardized policies, rigid routines, and a way of relating to individuals and their information that often becomes indifferent to their welfare.

The Interplay of the Metaphors. The Kafka and Orwell metaphors are not mutually exclusive. As I will discuss in more depth in part III of this book, the interplay of the metaphors captures the problems with government access to digital dossiers. In particular, the government is increasingly mining data from private-sector sources to profile individuals. Information about people is observed or recorded and then fed into computer programs that analyze the data looking for certain behavior patterns common to criminal or terrorist activity. This method of investigation and analysis employs secret **algorithms** to process information and calculate how “dangerous” or “criminal” a person might be. The results of these secret computations have palpable effects on people’s lives. People can be denied the right to fly on an airplane without a reason or a hearing; or they can be detained indefinitely without the right to an attorney and without being told the reasons why.

In another example, political scientist John Gilliom’s study of the surveillance of welfare recipients chronicles a world of constant observation coupled by an almost pathological bureaucracy.⁵² Recipients must fill out mountains of paperwork, answer endless questions, and be routinely monitored. Often, they receive so little financial assistance that they resort to odd jobs to obtain more income, which, if

discovered, could make them ineligible for benefits. The system creates a strong incentive for transgression, severe penalties for any breach, and elaborate data systems that attempt to detect any malfeasance through automated investigations. The system combines pervasive surveillance with a bureaucratic process that has little compassion or flexibility.

A quote by noted playwright and author Friedrich Dürrenmatt best captures how surveillance and bureaucracy interrelate in the Information Age:

[W]hat was even worse was the nature of those who observed and made a fool of him, namely a system of computers, for what he was observing was two cameras connected to two computers observed by two further computers and fed into computers connected to *those* computers in order to be scanned, converted, re-converted, and, after further processing by laboratory computers, developed, enlarged, viewed, and interpreted, by whom and where and whether at any point by human beings he couldn't tell.⁵³

Surveillance generates information, which is often stored in record systems and used for new purposes. Being watched and inhibited in one's behavior is only one part of the problem; the other dimension is that the data is warehoused for unknown future uses. This is where Orwell meets Kafka.

Beyond the Secrecy Paradigm

Understanding the database privacy problem in terms of the Kafka metaphor illustrates that the problem with databases concerns the use of information, not merely keeping it secret. Traditionally, privacy problems have been understood as invasions into one's hidden world. Privacy is about concealment, and it is invaded by watching and by public disclosure of confidential information. I refer to this understanding of privacy as the “secrecy paradigm.” This paradigm is so embedded in our privacy discourse that privacy is often represented visually by a roving eye, an open keyhole, or a person peeking through Venetian blinds.

Information about an individual, however, is often not secret, but is diffused in the minds of a multitude of people and scattered in various documents and computer files across the country. Few would be embarrassed by the disclosure of much of the material they read, the food they eat, or the products they purchase. Few would view their race, ethnicity, marital status, or religion as confidential. Of course, databases may contain the residue of scandals and skeletons—illicit websites, racy books, stigmatizing diseases—but since information in databases is rarely publicized, few reputations are tarnished. For the most part, the data is processed impersonally by computers without ever being viewed by the human eye. The secrecy paradigm focuses on breached confidentiality, harmed reputation, and unwanted publicity. But since these harms are not really the central problems of databases, privacy law often concludes that the information in databases is not private and is thus not entitled to protection. Indeed, one commentator defended DoubleClick's tracking of web browsing habits by stating:

Over time, people will realize it's not Big Brother who's going to show up [at]your door in a black ski mask and take your kids away or dig deep into your medical history. This is a situation where you are essentially dropped into a bucket with 40 million people who look and feel a lot like you do to the advertising company.⁵⁴

This commentator, viewing privacy with the Big Brother metaphor, focuses on the wrong types of harms and implicitly views only secret information as private.

The problem with databases pertains to the uses and practices associated with our information, not merely whether that information remains completely secret. Although disclosure can be a violation of privacy, this does not mean that avoiding disclosure is the sum and substance of our interest in privacy. What people want when they demand privacy with regard to their personal information is the ability to ensure that the information about them will be used only for the purposes they desire. Even regarding the Confidentiality of information, the understanding of privacy as secrecy fails to recognize that individuals want to keep things private from some people but not

others. The fact that an employee criticizes her boss to a co-worker does not mean that she wants her boss to know what she said.

Helen Nissenbaum, a professor of information technology, is quite right to argue that we often expect privacy even when in public.⁵⁵ Not all activities are purely private in the sense that they occur in isolation and in hidden corners. When we talk in a restaurant, we do not expect to be listened to. A person may buy condoms or hemorrhoid medication in a store open to the public, but certainly expects these purchases to be private activities. Contrary to the notion that any information in public records cannot be private, there is a considerable loss of privacy by plucking inaccessible facts buried in some obscure document and broadcasting them to the world on the evening news; Privacy can be infringed even if no secrets are revealed and even if nobody is watching us.

The Aggregation Effect

The digital revolution has enabled information to be easily amassed and combined. Even information that is superficial or incomplete can be quite useful in obtaining more data about individuals. Information breeds information. For example, although one's SSN does not in and of itself reveal much about an individual, it provides access to one's financial information, educational records, medical records, and a whole host of other information. As law professor Julie Cohen notes, "[a] comprehensive collection of data about an individual is vastly more than the sum of its parts."⁵⁶ I refer to this phenomenon as the "aggregation effect." Similar to a Seurat painting, where a multitude of dots juxtaposed together form a picture, bits of information when aggregated paint a portrait of a person.

In the Information Age, personal data is being combined to create a digital biography about us. Information that appears innocuous can sometimes be the missing link, the critical detail in one's digital biography, or the key necessary to unlock other stores of personal information. But why should we be concerned about a biography that includes details about what type of soap a person buys, whether she prefers Pepsi to Coca-Cola, or whether she likes to shop at Macy's rather than Kmart? As legal scholar Stan Karas points out, the prod-

ucts we consume are expressive of our identities.⁵⁷ We have many choices in the products we buy, and even particular brands symbolize certain personality traits and personal characteristics. Karas notes that Pepsi has marketed itself to a younger, more rebellious consumer than Coca-Cola, which emphasizes old-fashioned and traditional images in its advertisements.⁵⁸ Whether punk, yuppie, or hippie, people often follow a particular consumption pattern that reflects the subculture with which they identify.⁵⁹

Of course, the products we buy are not wholly reflective of our identities. A scene from Henry James's *Portrait of a Lady* best captures the complexities of the situation. Madame Merle, wise in the ways of the world yet jaded and selfish, is speaking to Isabel Archer, a young American lady in Europe full of great aspirations of living a bold and exceptional life, far beyond convention. Merle declares: "What shall we call our 'self'? Where does it begin? Where does it end? It overflows into everything that belongs to us—and then it flows back again. I know a large part of myself is the clothes I choose to wear. I've a great respect for *things!*" Isabel disagrees: "nothing that belongs to me is any measure of me." "My clothes only express the dressmaker," Isabel says, "but they don't express me. To begin with, it is not my own choice that I wear them; they've been imposed upon me by society."⁶⁰

Merle is obsessed by things, and she views herself as deeply intertwined with her possessions. The objects she owns and purchases are deeply constitutive of her personality. Isabel, in her proud individualism, claims that she is vastly distinct from what she owns and wears. Indeed, for her, things are a tool for conformity; they do not express anything authentic about herself.

Yet Madame Merle has a point—the information is indeed expressive. But Isabel is right, too—this information is somewhat superficial, and it only partially captures who we are. Although the digital biography contains a host of details about a person, it captures a distorted persona, one who is constructed by a variety of external details? Although the information marketers glean about us can be quite revealing, it still cannot penetrate into our thoughts and often only partially captures who we are.⁶² Information about our property, our professions, our purchases, our finances, and our medical history does not tell the whole story. We are more than the bits of data we give

off as we go about our lives. Our digital biography is revealing of ourselves but in a rather standardized way. It consists of bits of information pre-defined based on the judgment of some entity about what categories of information are relevant or important. We are partially captured by details such as our age, race, gender, net worth, property owned, and so on, but only in a manner that standardizes us into types or categories. Indeed, database marketers frequently classify consumers into certain categories based on stereotypes about their values, lifestyle, and purchasing habits. As Julie Cohen observes, people are not simply “reducible to the sum of their transactions, genetic markers, and other measurable attributes.”⁶³

Our digital biography is thus an unauthorized one, only partially true and very reductive. We must all live with these unauthorized biographies about us, the complete contents of which we often do not get to see. Although a more extensive dossier might be less reductive in capturing our personalities, it would have greater controlling effects on an individual’s life.

Not only are our digital biographies reductive, but they are often inaccurate. In today’s bureaucratized world, one of the growing threats is that we will be subject to the inadvertence, carelessness, and mindlessness of bureaucracy. A scene from the darkly humorous movie *Brazil* illustrates this problem.⁶⁴ The movie opens with an exhausted bureaucrat swatting a fly, which inconspicuously drops into a typewriter, causes a jam, and results in him mistyping a letter in a person’s name on a form. The form authorizes the arrest and interrogation of suspected rebels. In the next scene, an innocent man peacefully sits in his home with his family when suddenly scores of armor-clad police storm inside and haul him away.

These dangers are not merely the imaginary stuff of movies. The burgeoning use of databases of public record information by the private sector in screening job applicants and investigating existing employees demonstrates how errors can potentially destroy a person’s career. For example, a Maryland woman wrongly arrested for a burglary was not cleared from the state’s criminal databases. Her name and SSN also migrated to a Baltimore County database relating to child protective services cases. She was fired from her job as a substitute teacher, and only after she could establish that the information

was in error was she rehired. When she later left that job to run a day care center for the U.S. military, she was subjected to questioning about the erroneous arrest. Later on, when employed at as a child care director at a YMCA, she was terminated when her arrest record surfaced in a background clearance check. Since she could not have the error expunged in sufficient time, the job was given to another person. Only after several years was the error finally cleared from the public records.⁶⁵ As our digital biographies are increasingly relied upon to make important decisions, the problems that errors can cause will only escalate in frequency and magnitude.

To the extent that the digital biography is accurate, our lives are not only revealed and recorded, but also can be analyzed and investigated. Our digital biographies are being assembled by companies which are amassing personal information in public records along with other data. Collectively, millions of biographies can be searched, sorted, and analyzed in a matter of seconds. This enables automated investigations of individuals on a nationwide scale by both the government and the private sector. Increasingly, companies are conducting investigations which can have profound consequences on people's lives—such as their employment and financial condition. Employers are resorting to information brokers of public record information to assist in screening job applicants and existing employees. For example, the firm **HireCheck** serves over 4,000 employers to conduct background checks for new hires or current employees.⁶⁶ It conducts a national search of outstanding arrest warrants; a SSN search to locate the person's age, past and current employers, and former addresses; a driver record search; a search of worker's compensation claims "to avoid habitual claimants or to properly channel assignments"; a check of civil lawsuit records; and searches for many other types of information.⁶⁷ These investigations occur without any external oversight, and individuals often do not have an opportunity to challenge the results.

Forms of Dehumanization: Databases and the Kafka Metaphor

Expounding on the Kafka metaphor, certain uses of databases foster a state of powerlessness and vulnerability created by people's lack of

any meaningful form of participation in the collection and use of their personal information. Bureaucracy and power is certainly not a new problem. Databases do not cause the **disempowering** effects of bureaucracy; they exacerbate them—not merely by **magnifying** existing power imbalances but by transforming these relationships in profound **ways that** implicate our freedom. The problem is thus old and new, and its additional dimensions within the Information Age require extensive explication.

Impoverished Judgments. One of the great dangers of using information that we generally regard as private is that we often make judgments based on this private information about the person. As legal scholar Kenneth Karst warned in the 1960s, one danger of “a centralized, standardized data processing system” is that the facts stored about an individual “will become the only significant facts about the subject of the inquiry.”⁶⁸ Legal scholar Jeffrey Rosen aptly observes, “Privacy protects us from being **misdefined** and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge. True knowledge of another person is the culmination of a slow process of mutual revelation.”⁶⁹

Increased reliance upon the easily quantifiable and classifiable information available from databases is having profound social effects. The nature and volume of information affects the way people analyze, use, and react to information. Currently, we rely quite heavily on quantifiable data: statistics, polls, numbers, and figures. In the law alone, there is a trend to rank schools; to measure the influence of famous jurists by counting citations to their judicial opinions;⁷⁰ to assess the importance of law review articles by tabulating citations to them;⁷¹ to rank law journals with an elaborate system of establishing point values for authors of **articles**;⁷² and to determine the influence of academic movements by checking citations.⁷³ The goal of this use of empirical data is to eliminate the ambiguity and incommensurability of many aspects of life and try to categorize them into neat, tidy categories. The computer has exacerbated this tendency, for the increase in information and the way computers operate furthers this type of categorization and lack of judgment.⁷⁴ Indeed, in legal schol-

arship, much of this tendency is due to the advent of computer research databases, which can easily check for citations and specific terms.

In our increasingly bureaucratic and impersonal world, we are relying more heavily on records and profiles to assess reputation. As H. Jeff Smith; a professor of management and information technology, contends:

[D]ecisions that were formerly based on judgment and human factors are instead decided according to prescribed formulas. In today's world, this response is often characterized by reliance on a rigid, unyielding process in which computerized information is given great weight. Facts that actually require substantial evaluation could instead be reduced to discrete entries in preassigned categories.⁷⁵

Certainly, quantifiable information can be accurate and serve as the best way for making particular decisions. Even when quantifiable information is not exact, it is useful for making decisions because of administrative feasibility. Considering all the variables and a multitude of incommensurate factors might simply be impossible or too costly.

Nevertheless, the information in databases often fails to capture the texture of our lives. Rather than provide a nuanced portrait of our personalities, compilations of data capture the brute facts of what we do without the reasons. For example, a record of an arrest without the story or reason is misleading. The arrest could have been for civil disobedience in the 1960s—but it is still recorded as an arrest with some vague label, such as “disorderly conduct.” It appears no differently from the arrest of a vandal. In short, we are reconstituted in databases as a digital person composed of data. The privacy problem stems paradoxically from the pervasiveness of this data—the fact that it encompasses much of our lives—as well as from its limitations—how it fails to capture us, how it distorts who we are.

Powerlessness and Lack of Participation. Privacy concerns an individual's power in the elaborate web of social relationships that encompasses

her life. Today, a significant number of these relationships involve interaction with public and private institutions. In addition to the myriad of public agencies that regulate the products we purchase, the environment, and the like, we depend upon private institutions such as telephone companies, utility companies, Internet service providers, cable service providers, and health insurance companies. We also depend upon companies that provide the products we believe are essential to our daily lives: hygiene, transportation, entertainment, news, and so on. Our lives are ensconced in these institutions, which have power over our day-to-day activities (through what we consume, read, and watch), our culture, politics, education, and economic well-being. We are engaged in relationships with these institutions, even if on the surface our interactions with them are as rudimentary and distant as signing up for services, paying bills, and requesting repairs. With many firms—such as credit reporting agencies—we do not even take affirmative steps to establish a relationship.

Companies are beginning to use personal information to identify what business experts call “angel” and “demon” customers.⁷⁶ Certain customers—the angels—are very profitable, but others—the demons—are not. Angel customers account for a large amount of a company’s business whereas demon customers purchase only a small amount of goods and services and are likely to cost the company money. For example, a demon customer is one who uses up a company’s resources by frequently calling customer service. Some business experts thus recommend that companies identify these types of customers through the use of personal information and treat them differently. For example, businesses might serve the angels first and leave the demons waiting; or they might offer the angels cheaper prices; or perhaps, they might even try to turn the ~~demons~~ away entirely.” The result of companies moving in this direction is that people will be treated differently and may never know why. Even before the concept of angel and demon customers was articulated, one bank routinely denied credit card applications from college students majoring in literature, history, and art, based on the assumption that they would not be able to repay their debts. The bank’s practice remained a secret until the media ran a story about it.⁷⁸

We are increasingly not being treated as equals in our relationships with many private-sector institutions. Things are done to us; decisions are made about us; and we are often completely excluded from the process. With considerably greater frequency, we are ending up frustrated with the outcome. For example, complaints about credit reporting agencies to the Federal Trade Commission have been rapidly escalating, with 8,000 in 2001 and over 14,000 in 2002.⁷⁹

Privacy involves the ability to avoid the powerlessness of having others control information that can affect whether an individual gets a job, becomes licensed to practice in a profession, or obtains a critical loan. It involves the ability to avoid the collection and circulation of such powerful information in one's life without having any say in the process, without knowing who has what information, what purposes or motives those entities have, or what will be done with that information in the future. Privacy involves the power to refuse to be treated with bureaucratic indifference when one complains about errors or when one wants certain data expunged. It is not merely the collection of data that is the problem—it is our complete lack of control over the ways it is used or may be used in the future.

Problematic Information Gathering Techniques. This powerlessness is compounded by the fact that the process of information collection in America is clandestine, duplicitous, and unfair. The choices given to people over their information are hardly choices at all. People must relinquish personal data to gain employment, procure insurance, obtain a credit card, or otherwise participate like a normal citizen in today's economy. Consent is virtually meaningless in many contexts. When people give consent, they must often consent to a total surrender of control over their information.

Collection of information is often done by misleading the consumer. General Electric sent a supposedly anonymous survey to shareholders asking them to rate various aspects of the company. Unbeknownst to those surveyed, the survey's return envelope was coded so that the responses could be matched to names in the company's shareholder database.⁸⁰

Some information is directly solicited via registration questionnaires or other means such as competitions and sweepstakes. The

warranty registration cards of many products—which ask a host of lifestyle questions—are often sent not to the company that makes the product but to National Demographics and Lifestyles Company at a Denver post office box. This company has compiled information on over 20 million people and markets it to other companies.⁸¹ Often, there is an implicit misleading notion that consumers must fill out a registration questionnaire in order to be covered by the warranty.

Frequent shopper programs and discount cards—which involve filling out a questionnaire and then carrying a special card that provides discounts—enable the scanner data to be matched to data about individual consumers.⁸² This technique involves offering savings in return for personal information and the ability to track a person's grocery purchases.⁸³ However, there are scant disclosures that such an exchange is taking place, and there are virtually no limits on the use of the data.

Conde Nast Publications Inc. (which publishes the *New Yorker*, *Vanity Fair*, *Vogue*, and other magazines) recently sent out a booklet of 700 questions asking detailed information about an individual's hobbies, shopping preferences, health (including medications used, acne problems, and vaginal/yeast infections), and much more. Almost 400,000 people responded. In return for the data, the survey said: "Just answer the questions below to start the conversation and become part of this select group of subscribers to whom marketers listen first." Conde Nast maintains a database of information on 15 million people. Stephen Jacoby, the vice president for marketing and databases, said: "What we're trying to do is enhance the relationship between the subscriber and their magazine. In a sense, it's a benefit to the subscriber."⁸⁴

There is no "conversation" created by supplying the data. Conde Nast does not indicate how the information will be used. It basically tries to entice people to give information for a vague promise of little or no value. While the company insists that it will not share information with "outsiders," it does not explain who constitutes an "outsider." The information remains in the control of the company, with no limitations on use. Merely informing the consumer that data may be sold to others is an inadequate form of disclosure. The consumer

does not know how many times the data will be resold, to whom it will be sold, or for what purposes it will be used.

Irresponsibility and Carelessness. A person's lack of control is exacerbated by the often thoughtless and irresponsible ways that bureaucracies use personal information and their lack of accountability in using and protecting the data. In other words, the problem is not simply a lack of individual control over information, but a situation where *nobody* is exercising meaningful control over the information.

In bureaucratic settings, privacy policy tends to fall into drift and be reactionary. In a detailed study of organizations such as banks, insurance companies, and credit reporting agencies, H. Jeff Smith concluded that all of the organizations "exhibited a remarkably similar approach: the policy-making process, which occurred over time, was a wandering and reactive one." According to a senior executive at a health insurance company, "We've been lazy on the privacy [issues] for several years now, because we haven't had anybody beating us over the head about them." According to Smith, most executives in the survey were followers rather than leaders: "[M]ost executives wait until an external threat forces them to consider their privacy policies."⁸⁵

Furthermore, there have been several highly publicized instances where companies violated their own privacy policies. Although promising its users that their information would remain confidential, the website GeoCities collected and sold information about children who played games on the site.⁸⁶ **RealNetworks**, Inc. secretly collected personal information about its users in direct violation of its privacy policy. And a website for young investors promised that the data it collected about people's finances would remain anonymous, but instead it was kept in identifiable form.⁸⁷

More insidious than drifting and reactionary privacy policies are irresponsible and careless uses of personal information. For example, Metromail Corporation, a seller of direct marketing information, hired inmates to enter the information into databases. This came to light when an inmate began sending harassing letters that were sexually explicit and filled with intimate details of people's lives.⁸⁸ A television reporter once paid \$277 to obtain from Metromail a list of over

5,000 children living in Pasadena, California. The reporter gave the name of a well-known child molester and murderer as the buyer.⁸⁹ These cases illustrate the lack of care and accountability by the corporations collecting the data.

*McVeigh v. Cohen*⁹⁰ best illustrates this problem. A highly decorated 17-year veteran of the Navy sought to enjoin the Navy from discharging him under the statutory policy known as “Don’t Ask, Don’t Tell, Don’t Pursue.”⁹¹ When responding to a toy drive for the crew of his ship, Tim McVeigh (no relation to the Oklahoma City bomber) accidentally used the wrong email account, sending a message under the alias “boysrch.” He signed the email “Tim” but included no other information. The person conducting the toy drive searched through the member profile directory of America Online (AOL), where she learned that “boysrch” was an AOL subscriber named Tim who lived in Hawaii and worked in the military. Under marital status, he had identified himself as “gay.” The ship’s legal adviser began to investigate, suspecting that “Tim” was McVeigh. Before speaking to McVeigh, and without a warrant, the legal adviser had a paralegal contact AOL for more information. The paralegal called AOL’s toll-free customer service number and, without identifying himself as a Navy serviceman, concocted a story that he had received a fax from an AOL customer and wanted to confirm who it belonged to. Despite a policy of not giving out personal information, the AOL representative told him that the customer was McVeigh. As a result, the Navy sought to discharge McVeigh.

In *Remsburg v. Docusearch, Inc.*,⁹² a man named Liam Youens began purchasing information about Amy Lynn Boyer from a company called Docusearch. He requested Boyer’s SSN, and Docusearch obtained it from a credit reporting agency and provided it to him. Youens then requested Boyer’s employment address, so Docusearch hired a subcontractor, who obtained it by making a “pretext” phone call to Boyer. By lying about her identity and the reason for the call, the subcontractor obtained the address from Boyer. Docusearch then gave the address to Youens, who went to Boyer’s workplace and shot and killed her. Docusearch supplied the information without ever asking who Youens was or why he was seeking the information.

Within the past few years, explicit details of go psychotherapy patients’ sex lives, as well as their names, addresses, telephone num-

bers, and credit card numbers, were inadvertently posted on the Internet.⁹³ A banker in Maryland who sat on a state's public health commission checked his list of bank loans with records of people with cancer in order to cancel the loans of the cancer sufferers.⁹⁴ A hacker illegally downloaded thousands of patients' medical files along with their SSNs from a university medical center.⁹⁵ Due to a mix-up, a retirement plan mailed financial statements to the wrong people at the same firm.⁹⁶ Extensive psychological records describing the conditions of over 60 children were inadvertently posted on the University of Montana's website.⁹⁷ An employee of a company obtained 30,000 credit reports from a credit reporting agency and peddled them to others for use in fraud and identity theft.⁹⁸ Health information and SSNs of military personnel and their families were stolen from a military contractor's database.⁹⁹

In sum, the privacy problem created by the use of databases stems from an often careless and unconcerned bureaucratic process—one that has little judgment or accountability—and is driven by ends other than the protection of people's dignity. We are not just heading toward a world of Big Brother or one composed of Little Brothers, but also toward a more mindless process—of bureaucratic indifference, arbitrary errors, and dehumanization—a world that is beginning to resemble Kafka's vision in *The Trial*.

the digital person

Technology and Privacy in the Information Age

daniel j. solove

© 2004 by New York University



NEW YORK UNIVERSITY PRESS *New York and London*

2 The Rise of the Digital Dossier

We currently live in a world where extensive dossiers exist about each one of us. These dossiers are in digital format, stored in massive computer databases by a host of government agencies and **private-sector** companies. The problems caused by these developments are profound. But to understand the problems, we must first understand how they arose.

A History of Public-Sector Databases

Although personal records have been kept for centuries,¹ only in contemporary times has the practice become a serious concern. Prior to the nineteenth century, few public records were collected, and most of them were kept at a very local level, often by institutions associated with churches.² The federal government's early endeavors at collecting data consisted mainly in conducting the census. The first census in 1790 asked only four **questions**.³ With each proceeding census, the government gathered more personal information. By 1860, 142 questions were asked.⁴ When the 1890 census included questions about diseases, disabilities, and finances, it sparked a public outcry, ultimately leading to the passage in the early twentieth century of stricter laws protecting the confidentiality of census data.⁵

Government information collection flourished during the middle of the twentieth century. The creation and growth of government bureaucracy—spawning well over 100 federal agencies within the past century—led to an insatiable thirst for information about individuals. One such agency was the Social Security Administration, created in 1935, which assigned nine-digit numbers to each citizen and required extensive record-keeping of people's earnings.

Technology was a primary factor in the rise of information collection. The 1880 census required almost 1,500 clerks to tally information tediously by hand—and it took seven years to complete.⁶ At the rapid rate of population growth, if a faster way could not be found to tabulate the information, the 1890 census wouldn't be completed before the 1900 census began. Fortunately, just in time for the 1890 census, a census official named Herman Hollerith developed an innovative tabulating device—a machine that read holes punched in cards.⁷ Hollerith's new machine helped tabulate the 1890 census in under three years.⁸ Hollerith left the Census Bureau and founded a small firm that produced punch card machines—a firm that through a series of mergers eventually formed the company that became IBM.⁹

IBM's subsequent rise to prosperity was due, in significant part, to the government's increasing need for data. The Social Security System and other New Deal programs required a vast increase in records that had to be kept about individuals. As a result, the government became one of the largest purchasers of IBM's punch card machines.¹⁰ The Social Security Administration kept most of its records on punch cards, and by 1943 it had more than 100 million cards in storage.¹¹

The advent of the mainframe computer in 1946 revolutionized information collection. The computer and magnetic tape enabled the systematic storage of data. As processing speeds accelerated and as memory ballooned, computers provided a vastly increased ability to collect, search, analyze, and transfer records.

Federal and state agencies began to computerize their records. The Census Bureau was one of the earliest purchasers of commercially available computers.¹² Social Security numbers (SSNs)—originally not to be used as identifiers beyond the Social Security System—became immensely useful for computer databases.¹³ This is because SSNs en-

able data to be easily linked to particular individuals. In the 1970s, federal, state, and local governments—as well as the private sector—increasingly began to use them for identification.¹⁴

Beginning in the 1960s, the growing computerization of records generated a substantial buzz about privacy. Privacy captured the attention of the public, and a number of philosophers, legal scholars, and other commentators turned their attention to the threats to privacy caused by the rise of the computer.¹⁵ Congress began to debate how to respond to these emerging developments.¹⁶ In 1973, the U.S. Department of Health, Education, and Welfare (HEW) issued a report entitled *Records, Computers, and the Rights of Citizens*, which trenchantly articulated the growing concerns over computerized record systems:

There was a time when information about an individual tended to be elicited in face-to-face contacts involving personal trust and a certain symmetry, or balance, between giver and receiver. Nowadays, an individual must increasingly give information about himself to large and relatively faceless institutions, for handling and use by strangers—unknown, unseen, and, all too frequently, unresponsive. Sometimes the individual does not even know that an organization maintains a record about him. Often he may not see it, much less contest its accuracy, control its dissemination, or challenge its use by others.¹⁷

These problems continued to escalate throughout the ensuing decades. Computers grew vastly more powerful, and computerized records became ubiquitous. The rise of the Internet in the 1990s added new dimensions to these problems, sparking a revolution in the collection, accessibility, and communication of personal data.

Today, federal agencies and departments maintain almost 2,000 databases,¹⁸ including records pertaining to immigration, bankruptcy, licensing, welfare, and countless other matters. In a recent effort to track down parents who fail to pay child support, the federal government has created a vast database consisting of information about all people who obtain a new job anywhere in the nation. The database contains their SSNs, addresses, and wages.¹⁹

States maintain public records of arrests, births, criminal proceedings, marriages, divorces, property ownership, voter registration, workers' compensation, and scores of other types of records. State licensing regimes mandate that records be kept on numerous professionals such as doctors, lawyers, engineers, insurance agents, nurses, police, accountants, and teachers.

A History of Private-Sector Databases

Although the government played an integral role in the development of massive dossiers of personal information, especially early on, businesses soon began to play an even greater role. While the public-sector story concerns the quest for regulatory efficiency, the private-sector story involves money and marketing.

Long before the rise of nationwide advertising campaigns there was a personal relationship between merchant and customer. Local merchants lived next door to their customers and learned about their lives from their existence together in the community. To a large extent, marketing was done locally—by the peddler on the street or the shopkeeper on the corner. Mass marketing, which began in the nineteenth century and flourished in the twentieth century, transformed the nature of selling from personal one-to-one persuasion to large-scale advertising campaigns designed for the nameless, faceless American consumer.

Mass marketing consumed vast fortunes, and only a small fraction of the millions of people exposed to the ads would buy the products or services. Soon marketers discovered the power of a new form of marketing—targeted marketing. The idea was to figure out which people were most likely to consume a product and focus the advertising on them.

In the 1920s, the sales department of General Motors Corporation began an early experiment with targeted marketing. GM discovered that owners of Ford vehicles frequently didn't purchase a Ford as their next vehicle—so it targeted owners of two-year-old Fords and sent them a brochure on GM vehicles.²⁰ GM then began to send out questionnaires asking for consumer input into their products. GM be-

lied that this would be a good marketing device, presenting the image of a big corporation that cared enough to listen to the opinions of everyday people. GM cast itself as a democratic institution, its surveys stating that it was “OF THE PEOPLE, FOR THE PEOPLE, BY THE PEOPLE.” One GM print advertisement depicted a delighted child holding up the survey letter exclaiming: “Look dad, a letter from General Motors!” The campaign was quite successful—ironically not because of the data collected but because of GM’s image of appearing to be interested in the consumer’s ideas.²¹

Today, corporations are desperate for whatever consumer information they can glean, and their quest for information is hardly perceived as democratic. The data collected extends beyond information about consumers’ views of the product to information about the consumers themselves, often including lifestyle details and even a full-scale psychological profile.

The turn to targeting was spurred by the proliferation and specialization of mass media throughout the century, enabling marketers to tap into groups of consumers with similar interests and tastes. The most basic form of targeting involved selecting particular television programs, radio shows, or magazines in which to place advertisements. This technique, however, merely amounted to mass marketing on a slightly smaller scale.

The most revolutionary developments in targeted marketing occurred in the direct marketing industry. The practice of sending mail order catalogs directly to consumers began in the late nineteenth century when railroads extended the reach of the mail system.²² The industry also reached out to people by way of door-to-door salespersons. In the 1970s, marketers began calling people directly on the telephone, and “telemarketing” was born.

Direct marketing remained a fledgling practice for most of the twentieth century. Direct marketers had long accepted the “2 percent” rule—only 2 percent of those contacted would respond.²³ With such a staggering failure rate, direct marketing achieved its successes at great cost. To increase the low response rate, marketers sought to sharpen their targeting techniques, which required more consumer research and an effective way to collect, store, and analyze information

about consumers. The advent of the computer database gave marketers this long sought-after ability—and it launched a revolution in targeting technology.

Databases provided an efficient way to store and search for data. Organized into fields of information, the database enabled marketers to sort by various types of information and to rank or select various groups of individuals from its master list of customers—a practice called “modeling.” Through this process, fewer mailings or calls needed to be made, resulting in a higher response rate and lower costs. In addition to isolating a company’s most profitable customers, marketers studied them, profiled them, and then used that profile to find similar customers.²⁴ This, of course, required not only information about existing customers, but the collection of data about prospective customers as well.

Originally, marketers sought to locate the best customers by identifying those customers who purchased items most recently and frequently and who spent the most money.²⁵ In the 1970s, marketers turned to demographic information.²⁶ Demographics included basic information such as age, income level, race, ethnicity, gender, and geographical location. Marketers could target certain demographic segments of the nation, a practice called “cluster marketing.” This approach worked because people with similar incomes and races generally lived together in clusters.

The private sector obtained this demographic information from the federal government. In the 1970s, the United States began selling its census data on magnetic tapes. To protect privacy, the Census Bureau sold the information in clusters of 1,500 households, supplying only addresses—not names. But clever marketing companies such as Donnelley, Metromail, and R. L. Polk reattached the names by matching the addresses with information in telephone books and voter registration lists. Within five years of purchasing the census data, these companies had constructed demographically segmented databases of over half of the households in the nation.²⁷

In the 1980s, marketers looked to supplement their data about consumers by compiling “psychographic” information—data about psychological characteristics such as opinions, attitudes, beliefs, and lifestyles.²⁸ For example, one company established an elaborate tax-

onomy of people, with category names such as “Blue Blood Estates,” “BohemianMix,” “YoungLiterati,” “Shotguns and Pickups,” and “Hispanic Mix.”²⁹ Each cluster had a description of the type of person, their likes, incomes, race and ethnicity, attitudes, and hobbies.³⁰

These innovations made targeted marketing—or “database marketing” as it is often referred to today—the hottest form of marketing, growing at twice the rate of America’s gross national product.³¹ In 2001, direct marketing resulted in almost \$2 trillion in sales.³² On average, over 500 pieces of unsolicited advertisements, catalogs, and marketing mailings arrive every year at each household.³³ Due to targeting, direct mail yields \$10 in sales for every \$1 in cost—a ratio double that for a television advertisement—and forecasters predict catalog sales will grow faster than retail sales.³⁴ Telemarketing is a \$662 billion a year industry.³⁵ In a 1996 Gallup poll, 77 percent of U.S. companies used some form of direct mail, targeted email, or telemarketing.³⁶

The effectiveness of targeted marketing depends upon data, and the challenge is to obtain as much of it as possible. Marketers discovered that they didn’t have to research and collect all the information from scratch, for data is the perspiration of the Information Age. Billions of bytes are released each second as we click, charge, and call. A treasure trove of information already lay untapped within existing databases, retail records, mailing lists, and government records. All that marketers had to do was plunder it as efficiently as possible.

The increasing thirst for personal information spawned the creation of a new industry: the database industry, an Information Age bazaar where personal data collections are bartered and sold. Marketers “rent” lists of names and personal information from database companies, which charge a few cents to a dollar for each name.³⁷ Over 550 companies compose the personal information industry, with annual revenues in the billions of dollars.³⁸ The sale of mailing lists alone (not including the sales generated by the use of the lists) generates \$3 billion a year.³⁹ The average consumer is on around 100 mailing lists and is included in at least 50 databases.⁴⁰

An increasing number of companies with databases—magazines, credit card companies, stores, mail order catalog firms, and even telephone companies—are realizing that their databases are becoming one of their most valuable assets and are beginning to sell their data.

A new breed of company is emerging that devotes its primary business to the collection of personal information. Based in Florida, Catalina Marketing Corporation maintains supermarket buying history databases on 30 million households from more than 5,000 stores.⁴¹ This data contains a complete inventory of one's groceries, over-the-counter medications, hygiene supplies, and contraceptive devices, among others. Aristotle, Inc. markets a database of 150 million registered voters. Aristotle's database records voters' names, addresses, phone numbers, party affiliation, and voting frequency. Aristotle combines this data with about 25 other categories of information, such as one's race, income, and employer—even the make and model of one's car. It markets a list of wealthy campaign donors called "Fat Cat." Aristotle boasts: "Hit your opponent in the Wallet! Using Fat Cats, you can ferret out your adversary's contributors and slam them with a mail piece explaining why they shouldn't donate money to the other side."⁴² Another company manufactures software called **GeoVoter**, which combines about 5,000 categories of information about a voter to calculate how that individual will

The most powerful database builders construct information empires, sometimes with information on more than half of the American population. For example, Donnelley Marketing Information Services of New Jersey keeps track of 125 million people. Wiland Services has constructed a database containing over 1,000 elements, from demographic information to behavioral data, on over 215 million people. There are around five database compilers that have data on almost all households in the United States.⁴³

Beyond marketers, hundreds of companies keep data about us in their record systems. The complete benefits of the Information Age do not simply come to us—we must "plug in" to join in. In other words, we must establish relationships with Internet Service Providers, cable companies, phone companies, insurance companies, and so on. All of these companies maintain records about us. The Medical Information Bureau, a nonprofit institution, maintains a database of medical information on 15 million individuals, which is available to over 700 insurance companies.⁴⁵ Credit card companies have also developed extensive personal information databases. Un-

like cash, which often does not involve the creation of personally identifiable records, credit cards result in detailed electronic documentation of our purchases.⁴⁶

Increasingly, we rely on various records and documents to assess financial reputation.⁴⁷ According to sociologist Steven Nock, this enables reputations to become portable.⁴⁸ In earlier times, a person's financial condition was generally known throughout the community. In modern society, however, people are highly mobile and creditors often lack first-hand experience of the financial condition and trustworthiness of individuals. Therefore, creditors rely upon credit reporting agencies to obtain information about a person's credit history. Credit reports reveal a person's consistency in paying back debts as well as the person's loan defaulting risk. People are assigned a credit score, which impacts whether they will be extended credit, and, if so, what rate of interest will be charged. Credit reports contain a detailed financial history, financial account information, outstanding debts, bankruptcy filings, judgments, liens, and mortgage foreclosures. Today, there are three major credit reporting agencies—Equifax, Experian, and Trans Union. Each agency has compiled extensive dossiers about almost every adult U.S. citizen.⁴⁹ Credit reports have become essential to securing a loan, obtaining a job, purchasing a home or a car, applying for a license, or even renting an apartment. Credit reporting agencies also prepare investigative consumer reports, which supplement the credit report with information about an individual's character and lifestyle.⁵⁰

Launched in 2002, Regulatory DataCorp (RDC) has created a massive database to investigate people opening new bank accounts. RDC was created by many of the world's largest financial companies. Its database, named the Global Regulatory Information Database (GRID), gathers information from over 20,000 different sources around the world.⁵¹ RDC's purpose is to help financial companies conduct background checks of potential customers for fraud, money laundering, terrorism, and other criminal activity. Although some people's information in the database may be incorrect, they lack the ability to correct the errors. RDC's CEO and president responds: "There are no guarantees. Is the public information wrong? We don't have enough information to say it's wrong."⁵²

Cyberspace and Personal Information

Cyberspace is the new frontier for gathering personal information, and its power has only begun to be exploited. The Internet is rapidly becoming the hub of the personal information market, for it has made the peddling and purchasing of data much easier. Focus USA's website boasts that it has detailed information on 203 million people.⁵³ Among its over 100 targeted mailing lists are lists of "Affluent Hispanics," "Big-Spending Parents," "FirstTime Credit Card Holders," "Grown But Still At Home," "Hi-Tech Seniors," "New Homeowners," "Status Spenders," "Big Spending Vitamin Shoppers," and "Waist Watchers."⁵⁴ For example, Focus USA states for its list of "New Movers":

As much as 20% of the population moves every year. . . . New movers have a lot of needs in their first few months. . . . During this lifestyle change period, new movers tend to be more receptive to direct mail and telemarketing offers for a wide variety of products.

The database contains data about age, gender, income, children, Internet connections, and more. There is a list devoted exclusively to "NewMovers With Children," which includes data on the ages of the children. A list called "Savvy Single Women" states that "[s]ingle women represent a prime market for travel/vacation, frequent flyer clubs, credit cards, investing, dining out, entertainment, insurance, catalog shopping, and much more."

There's also a list of "Mr.Twenty Somethings" that contains mostly college-educated men who Focus USA believes are eager to spend money on electronic equipment. And there are lists of pet lovers, fitness-conscious people, cat and dog owners, motorcycle enthusiasts, casino gamblers, opportunity seekers, and sub-prime prospects.⁵⁵ Dunhill International also markets a variety of lists, including "America's Wealthiest Families," which includes 9.6 million records "appended with demographic and psychographic data."⁵⁶ There are also databases of disabled people, consumers who recently applied for a credit card, cruise ship passengers, teachers, and couples who just had a baby. Hippo Direct markets lists of people suffering from "med-

ical maladies” such as constipation, cancer, diabetes, heart disease, impotence, migraines, enlarged prostate, and more.⁵⁷ Another company markets a list of 5 million elderly incontinent women.⁵⁸ In addition to serving as a marketplace for personal information, cyberspace has provided a revolution for the targeted marketing industry because web pages are not static—they are generated every time the user clicks. Each page contains spaces reserved for advertisements, and specific advertisements are downloaded into those spots. The dynamic nature of web pages makes it possible for a page to download different advertisements for different users.

Targeting is very important for web advertising because a web page is cluttered with information and images all vying for the users’ attention. Similar to the response rates of earlier efforts at direct marketing, only a small percentage of viewers (about 2 percent) click the advertisements they view.⁵⁹ The Internet’s greater targeting potential and the fierce competition for the consumer’s attention have given companies an unquenchable thirst for information about web users. This information is useful in developing more targeted advertising as well as in enabling companies to better assess the performance and popularity of various parts of their **websites**.

Currently, there are two basic ways that websites collect personal information. First, many websites directly solicit data from their users. **Numerous websites** require users to register and log in, and registration often involves answering a questionnaire. Online merchants amass data from their business transactions with consumers. For example, I shop on Amazon.com, which keeps track of my purchases in books, videos, music, and other items. I can view its records of every item I’ve ever ordered, and this goes back well over six years. When I click on this option, I get an alphabetized list of everything I bought and the date I bought it. **Amazon.com** uses its extensive records to recommend new books and videos. With a click, I can see dozens of books that **Amazon.com** thinks I’ll be interested in. It is eerily good, and it can pick out books for me better than my relatives can. It has me pegged.

Websites can also secretly track a customer’s **websurfing**. When a person explores a website, the website can record data about her ISP, computer hardware and software, the website she linked from, and

exactly what parts of the website she explored and for how long. This information is referred to as “clickstream data” because it is a trail of how a user navigates throughout the web by clicking on various links. It enables the website to calculate how many times it has been visited and what parts are most popular. With a way to connect this information to particular web users, marketers can open a window into people’s minds. This is a unique vision, for while marketers can measure the size of audiences for other media such as television, radio, books, and magazines, they have little ability to measure attention span. Due to the interactive nature of the Internet, marketers can learn how we respond to what we hear and see. A website collects information about the way a user interacts with the site and stores the information in its database. This information will enable the website to learn about the interests of a user so it can better target advertisements to the user. For example, [Amazon.com](#) can keep track of every book or item that a **customer** browses but does not purchase.

To connect this information with particular users, a company can either require a user to log in or it can secretly tag a user to recognize her when she returns. This latter form of identification occurs through what is called a “cookie.” A cookie is a small text file of codes that is deployed into the user’s computer when she downloads a web page.⁶⁰ Websites place a unique identification code into the cookie, and the cookie is saved on the user’s hard drive. When the user visits the site again, the site looks for its cookie, recognizes the user, and locates the information it collected about the user’s previous surfing activity in its database. Basically, a cookie works as a form of high-tech cattle-branding.

Cookies have certain limits. First, they often are not tagged to particular individuals—just to particular computers. However, if the website requires a user to log in or asks for a name, then the cookies will often contain data **identifying** the individual. Second, typically, websites can only decipher the cookies that they placed on a user’s computer; they cannot use cookies stored by a different website.

To get around these limitations, companies have devised strategies of information sharing with other websites. One of the most popular information sharing techniques is performed by a firm called DoubleClick. When a person visits a website, it often takes a quick detour

to Doubleclick. Doubleclick accesses its cookie on the person's computer and looks up its profile about the person. Based on the profile, Doubleclick determines what advertisements that person will be most responsive to, and these ads are then downloaded with the website the person is accessing. All this occurs in milliseconds, without the user's knowledge. Numerous websites subscribe to Doubleclick. This means that if I click on the same website as you at the very same time, we will receive different advertisements calculated by DoubleClick to match our interests. People may not know it, but DoubleClick cookies probably reside on their computer. As of the end of 1999, Doubleclick had amassed 80 million customer profiles.⁶¹

Another information collection device, known as a "web bug," is embedded into a web page or even an email message. The web bug is a hidden snippet of code that can gather data about a person.⁶² For example, a company can send a spam email with a web bug that will report back when the message is opened. The bug can also record when the message is forwarded to others. Web bugs also can collect information about people as they explore a website. Some of the nastier versions of web bugs can even access a person's computer files.⁶³

Companies also use what has become known as "spyware," which is software that is often deceptively and secretly installed into people's computers. Spyware can gather information about every move one makes when surfing the Internet. This data is then used by spyware companies to target pop-up ads and other forms of advertising.⁶⁴

Legal scholar Julie Cohen has noted another growing threat to privacy—technologies of digital rights management (DRM), which are used by copyright holders to prevent piracy. Some DRM technologies gather information about individuals as they listen to music, watch videos, or read e-books. DRM technologies thus "create records of intellectual exploration, one of the most personal and private of activities."⁶⁵

Copyright holders are also using computer programs called "bots" (shorthand for "robots"). Also known as "crawlers" or "spiders," bots can automatically prowl around the Internet looking for information. Industry trade groups, such as the Recording Industry Association of America (RIAA) and the Motion Picture Association of America

(MPAA), have unleashed tens of thousands of bots to identify potential illegal users of copyrighted materials.⁶⁶ Spammers—the senders of junk email—also employ a legion of bots to copy down email addresses that appear on the web in order to add them to spam lists. Bots also patrol Internet chat rooms, hunting for data.⁶⁷

As we stand at the threshold of an age structured around information, we are only beginning to realize the extent to which our lives can be encompassed within its architecture. “The time will come,” predicts one marketer, “when we are well known for our inclinations, our predilections, our proclivities, and our wants. We will be classified, profiled, categorized, and our every click will be watched.”⁶⁸ As we live more of our lives on the Internet, we are creating a permanent record of unparalleled pervasiveness and depth. Indeed, almost everything on the Internet is being archived. One company has even been systematically sweeping up all the data from the Internet and storing it in a vast electronic warehouse.⁶⁹ Our online personas—captured, for instance, in our web pages and online postings—are swept up as well. We are accustomed to information on the web quickly flickering in and out of existence, presenting the illusion that it is ephemeral. But little on the Internet disappears or is forgotten, even when we delete or change the information. The amount of personal information archived will only escalate as our lives are increasingly digitized into the electric world of cyberspace.

These developments certainly suggest a threat to privacy, but what specifically is the problem? The way this question is answered has profound implications for the way the law will grapple with the problem in the future.

Landmarks

The Case That Started It All: *Roberson v. The Rochester Folding Box Company*

VICTORIA PRUSSEN SPEARS

More than a century ago, New York's highest court, the Court of Appeals, was asked to find a right to privacy in a case brought by a young woman whose portrait had been used, without her prior consent, in an advertisement for a flour company. The court rejected the request — but its ruling was following by public outrage that led the state's legislature to promptly enact a statute creating a right to privacy that exists to this very day.

Abram Lincoln is famously said to have exclaimed to Harriet Beecher Stowe, the author of “Uncle Tom’s Cabin,” when he met her in 1862, “So this is the little lady who started our big war!” On some level, it might be said that Abigail M. Roberson is the young girl who started our country’s privacy revolution, which began when a case bearing her name, *Roberson v. The Rochester Folding Box Company*,¹ was decided by New York’s highest court, the Court of Appeals, more

Victoria Prusen Spears is an attorney in Miller Place, N.Y. She may be contacted at victoriapspears@aol.com.

than a century ago, in 1902. Although a divided court actually ruled against the plaintiff, the New York State Legislature soon took up the cause, leading to a statutory privacy right in New York that continues to exist to this day.²

FLOUR POWER

The complaint filed on behalf of Abigail Roberson alleged that the Franklin Mills Co., which was engaged in the business of milling and in the manufacture and sale of flour, obtained, made, printed, sold and circulated about 25,000 lithographic prints, photographs, and likenesses of Abigail without her prior knowledge or consent. The complaint also alleged that the company had printed on those papers, in large, plain letters, the words, "Flour of the Family," and below Abigail's portrait in large capital letters, "Franklin Mills Flour." In addition, the lower right hand corner, in smaller capital letters, stated, "Rochester Folding Box Co., Rochester, N.Y." According to the complaint, the sheets advertised Franklin Mills' flour, and the 25,000 sheets were "conspicuously posted and displayed in stores, warehouses, saloons and other public places." The complaint further asserted that they had been recognized by friends of the plaintiff and other people with the result that she had been "greatly humiliated by the scoffs and jeers" of people who recognized her face and picture on this advertisement and "her good name" had been attacked, causing her "great distress and suffering both in body and mind." The complaint alleged that this had made Abigail sick and that she had "suffered a severe nervous shock, was confined to her bed and compelled to employ a physician." She sought \$15,000 in damages and asked that Franklin Mills and the Rochester Folding Box Co. be enjoined from making, printing, publishing, circulating, or using in any manner any likenesses of her in any form whatever.

The trial court overruled demurrers to the complaint and entered judgment in favor of the plaintiff. The decision of an intermediate appellate court stated, in part, "It may be said in the first place that the theory upon which this action is predicated is new, at least in instance if not in principle, and that few precedents can be found to sustain the claim made

by the plaintiff, if indeed it can be said that there are any authoritative cases establishing her right to recover in this action.” That appellate court nevertheless reached the conclusion that the plaintiff had a good cause of action against the defendants, in that the defendants had invaded what the appellate court characterized as the plaintiff’s “right of privacy.” The case reached the New York Court of Appeals, which reversed, 4-3.

THE COURT OF APPEALS’ MAJORITY DECISION

The majority opinion pointed out that the plaintiff did not allege that she had been libeled by the publication of her portrait — the likeness was “said to be a very good one, and one that her friends and acquaintances were able to recognize.” Indeed, the court noted, the plaintiff’s grievance was that a good portrait of her, and, therefore, one easily recognized, had been used to attract attention toward the paper on which the mill company’s advertisements appeared. That publicity was “very distasteful” to the plaintiff, and thus, because of the defendants’ use of her picture without her consent for their own business purposes, she had “been caused to suffer mental distress.” The Court noted that some people would have found this publicity “agreeable” and “would have appreciated the compliment to their beauty implied in the selection of the picture for such purposes.”

The majority continued by declaring that there was “no precedent” for an action by the plaintiff in this situation “to be found in the decisions of this court.” It continued by observing that the “right to be let alone” was not a right found “in Blackstone, Kent or any other of the great commentators upon the law.” Moreover, the majority stated, its existence did not seem to have been asserted prior to about the year 1890, “when it was presented with attractiveness and no inconsiderable ability in the Harvard Law Review (Vol. IV, page 193) in an article [by Samuel D. Warren and Louis D. Brandeis] entitled, ‘The Right of Privacy.’”

According to the court, the “so-called right of privacy” was “founded upon the claim that a man has the right to pass through this world, if he wills, without having his picture published, his business enterprises discussed, his successful experiments written up for the benefit of others, or his eccentricities commented upon” in “handbills, circulars, cata-

logues, periodicals or newspapers," and "that the things which may not be written and published of him must not be spoken of him by his neighbors, whether the comment be favorable or otherwise." The Court stated that although "most persons" would "much prefer to have a good likeness of themselves appear in a responsible periodical or leading newspaper rather than upon an advertising card or sheet," the doctrine that the plaintiff asked the courts to create for this case "would apply as well to the one publication as to the other," because the principle on which the plaintiff asked the courts to base her recovery in this action was that:

the right of privacy exists and is enforceable in equity, and that the publication of that which purports to be a portrait of another person, even if obtained upon the street by an impertinent individual with a camera, will be restrained in equity on the ground that an individual has the right to prevent his features from becoming known to those outside of his circle of friends and acquaintances.

The Court stated that if such a principle were to be incorporated into the law through a court of equity, "the attempts to logically apply the principle will necessarily result, not only in a vast amount of litigation, but in litigation bordering upon the absurd." The Court said that was because the right of privacy, once established as a legal doctrine, could not be confined "to the restraint of the publication of a likeness but must necessarily embrace as well the publication of a word-picture, a comment upon one's looks, conduct, domestic relations or habits." Were the right of privacy legally asserted, it would "necessarily" be held to include the same things "if spoken instead of printed, for one, as well as the other, invades the right to be absolutely let alone." An "insult," the court stated, would certainly be in violation of such a right, and many persons would more seriously object to that than to the publication of their picture. Pointing out that there were many things that were "spoken and done day by day" that "seriously offend the sensibilities of good people," the court declared that "the vast field of litigation" would "necessarily be opened up" should it hold that privacy exists "as a legal right enforceable in equity by injunction, and by damages where they seem necessary to

give complete relief.”

It recognized that the intermediate appellate court had stated that it was not the rule that the absence of a precedent was “a sufficient reason for turning the plaintiff out of court.” The court added, however, that that was so only if “there can be found a clear and unequivocal principle of the common law which either directly or mediately governs it or which by analogy or parity of reasoning ought to govern it.”

The court then examined whether the right of privacy as a legal doctrine enforceable in equity had been established by prior court opinions. Examining a variety of decisions, it concluded that the “so-called ‘right of privacy’” had not as of then found a place in its jurisprudence, and therefore the doctrine could not be incorporated “without doing violence to settled principles of law by which the profession and the public have long been guided.”

The court concluded by stating that it was not declaring that a party whose likeness was circulated against his or her will was without remedy in every case. It noted that under then-Section 245 of the Penal Code, any malicious publication (meaning simply “intentional and willful”) by picture, effigy or sign that exposed a person to “contempt, ridicule or obloquy” was a libel, and would constitute such at common law. It noted that there were many products, especially medical products, whose character was such that using the picture of a person, “particularly that of a woman,” in connection with the advertisement of those items “might justly be found by a jury to cast ridicule or obloquy on the person whose picture was thus published.” Moreover, the “manner or posture” in which a person was portrayed might readily have a like effect. “In such cases both a civil action and a criminal prosecution could be maintained,” the court stated. It then reversed the judgment of the intermediate appellate court.

THE DISSENT

Three members of the court dissented, declaring in part that permitting a portrait to be put to “commercial, or other, uses for gain, by the publication of prints therefrom” was an act of invasion of the individual’s privacy, “possibly more formidable and more painful in its consequences,

than an actual bodily assault might be.” The minority stated that the security of a person was “as necessary as the security of property” and that for complete personal security, “which will result in the peaceful and wholesome enjoyment of one’s privileges as a member of society, there should be afforded protection, not only against the scandalous portraiture and display of one’s features and person, but against the display and use thereof for another’s commercial purposes or gain.” Simply put, the dissent concluded that the plaintiff had the right “to be protected against the use of her face for defendant’s commercial purposes,” and that that right did not depend upon the existence of property.

A STATUTORY RIGHT

Interestingly, the court’s majority observed that the legislature “could very well interfere and arbitrarily provide that no one should be permitted for his own selfish purpose to use the picture or the name of another for advertising purposes without his consent.” That’s what the New York State Legislature did when it enacted Section 50 and Section 51 of the state’s Civil Rights Law following a public uproar after the court’s decision. Section 50 essentially incorporates the dissent’s view of the plaintiff’s lawsuit and the majority’s observation about a statute that the legislature could enact. Section 50 now states:

Right of privacy. A person, firm or corporation that uses for advertising purposes, or for the purposes of trade, the name, portrait or picture of any living person without having first obtained the written consent of such person, or if a minor of his or her parent or guardian, is guilty of a misdemeanor.

Thus, the use of a living person’s “name, portrait or picture” for commercial purposes without prior written consent is a crime in New York. Section 51 grants an individual in such a situation the right to obtain an injunction and damages — including in appropriate circumstances, punitive damages. It currently states:

Action for injunction and for damages. Any person whose name, portrait, picture or voice is used within this state for advertising purposes or for the purposes of trade without the written consent first obtained as above provided may maintain an equitable action in the supreme court of this state against the person, firm or corporation so using his name, portrait, picture or voice, to prevent and restrain the use thereof; and may also sue and recover damages for any injuries sustained by reason of such use and if the defendant shall have knowingly used such person's name, portrait, picture or voice in such manner as is forbidden or declared to be unlawful by section fifty of this article, the jury, in its discretion, may award exemplary damages. But nothing contained in this article shall be so construed as to prevent any person, firm or corporation from selling or otherwise transferring any material containing such name, portrait, picture or voice in whatever medium to any user of such name, portrait, picture or voice, or to any third party for sale or transfer directly or indirectly to such a user, for use in a manner lawful under this article; nothing contained in this article shall be so construed as to prevent any person, firm or corporation, practicing the profession of photography, from exhibiting in or about his or its establishment specimens of the work of such establishment, unless the same is continued by such person, firm or corporation after written notice objecting thereto has been given by the person portrayed; and nothing contained in this article shall be so construed as to prevent any person, firm or corporation from using the name, portrait, picture or voice of any manufacturer or dealer in connection with the goods, wares and merchandise manufactured, produced or dealt in by him which he has sold or disposed of with such name, portrait, picture or voice used in connection therewith; or from using the name, portrait, picture or voice of any author, composer or artist in connection with his literary, musical or artistic productions which he has sold or disposed of with such name, portrait, picture or voice used in connection therewith. Nothing contained in this section shall be construed to prohibit the copyright owner of a sound recording from disposing of, dealing in, licensing or selling that sound recording to any party, if the right to dispose of,

deal in, license or sell such sound recording has been conferred by contract or other written document by such living person or the holder of such right. Nothing contained in the foregoing sentence shall be deemed to abrogate or otherwise limit any rights or remedies otherwise conferred by federal law or state law.

The New York Court of Appeals has had further opportunities to find in favor of a common law right to privacy in the state, but, following *Roberson*, has refused to do so. Nonetheless, Section 50 and 51 have been relied on by individuals, frequently, to protect their privacy rights. It of course is not clear when, if at all, the statutes would have been adopted had *Roberson* not reached the court and had the court's ruling not generated such a fierce public response. But privacy, under Sections 50 and 51, is well established in New York. And it all derives from an advertisement for flour that used a young girl's picture, without her consent.

NOTES

¹ 171 N.Y. 538 (1902).

² See New York Civil Rights Law Sections 50 and 51.

Three Common Privacy Misconceptions That Companies Love

Privacy-invading companies love it that people feel helpless, but now is the time for people to trade resignation for activism.

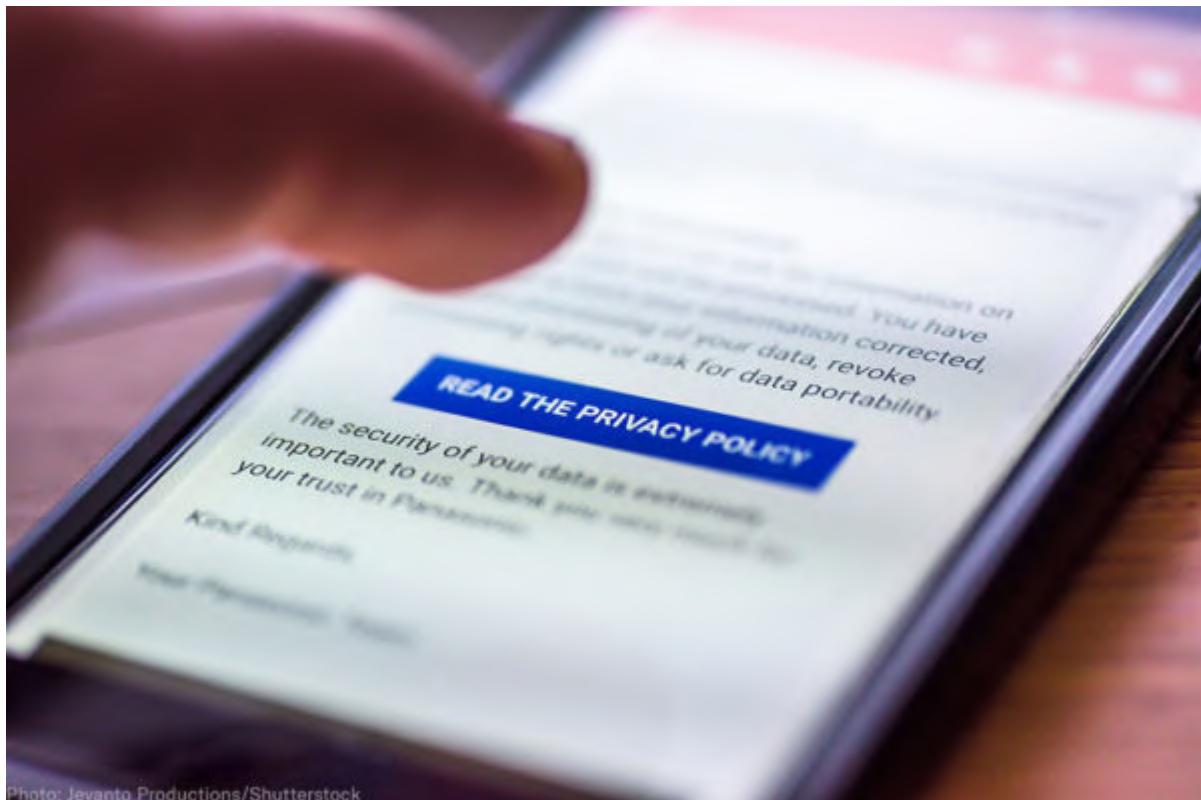


Photo: Jevanto Productions/Shutterstock

Jay Stanley, Senior Policy Analyst

November 14, 2019

A significant number of Americans hold significant misconceptions about their privacy, according to opinion research — misconceptions that privacy-invading companies love. That's according to research on American understandings of privacy carried out over the past couple decades by the Annenberg School for Communication at the University of Pennsylvania, lead by Prof. Joseph Turow, whom I recently heard give a [talk](#) summarizing these studies.

Misconception #1: "We care about your privacy!"

One misconception is that when a web site has a “privacy policy,” that actually means the site has a policy to protect your privacy. Annenberg presented respondents with the false statement that “When a web site has a privacy policy, it means the site will not share my information with other websites or companies without my permission.” In 2018, nearly 60 percent of Americans either said they believed this was true, or that they did not know. In [past years](#) the percentage of those surveyed giving incorrect answers was as high as 78 percent.

Unfortunately, nothing could be further from the truth. Most “privacy” policies start by declaring, “We care about your privacy!” and then go on to say, in extremely long and complicated legal language, that you have no privacy. Lawyers write these policies to minimize the presence of any actual concrete promises that might limit what a company does. Because the United States doesn’t yet have a baseline privacy law, the only thing protecting our privacy in most commercial contexts is a prohibition on “acts or practices that are unfair or deceptive.” That prohibition was [enacted](#) in 1914 — just *slightly* before the advent of today’s online advertising surveillance systems. What that means is that (outside of a few narrow areas that are regulated such as credit reporting) a company can do whatever it wants with your personal information. The only thing it generally cannot do under federal law is *say* it’s going to do one thing and then do another, which would count as “unfair or deceptive,” and leave a company vulnerable to enforcement by the Federal Trade Commission.

Turow says that “marketers know” about this misconception and benefit from the confusion and the misplaced consumer trust it creates. Turow suggests that “privacy policy” is “a deceptive term” and that “the FTC should require a change in the label.” “How We Use Your Data” would be more accurate.

Misconception #2: What is unfair is also illegal.

A second misconception that many Americans hold is that the law protects them more than it does. For example, in 2015, 62 percent of Americans didn’t know that it is completely legal for an online store to “charge different prices to different people at the same time of day”; in 2012, 76 percent did not know that “online marketers are allowed to share information about diseases you or your family members have”; and in 2018, 46 percent did not know that an “internet provider has a legal right to sell information to marketers about the websites you visit.” (We

think they actually *don't* have such a right under the Communications Act, which states that “every telecommunications carrier has a duty to protect the confidentiality” of personal information — but an [attempt](#) to craft detailed rules enforcing that law was [killed](#) by Congress and President Trump in 2017, and there’s no sign that such a right will be enforced by the federal government anytime soon.)

What’s going on here, Turow believes, is that people have fairly well-defined feelings about what kinds of behavior are fair and what are not — and they tend to think that things that are unfair are also illegal. They think, as he puts it, that the government has our backs much more than it actually does.

Annenberg’s polling confirms other [polling](#) in [consistently finding](#) that people are deeply uncomfortable with the state of their privacy online. Two-thirds (66 percent) of adults, for example, told surveyors that they do not want advertisements “tailored to their interests,” and 91 percent disagreed with the statement that “if companies give me a discount, it is a fair exchange for them to collect information about me without my knowing.” Asked whether “It’s okay if a store where I shop uses information it has about me to create a picture of me that improves the services they provide for me,” 55 percent disagreed.

These findings, Turow concludes, “refute marketers’ insistence that Americans find increased personalized surveillance and targeting for commercial purposes acceptable.”

So why do people give up so much information? The problem is that they feel helpless. The surveys found that 58 percent of Americans agreed with the statement, “I want to have control over what marketers can learn about me online” — but at the same time 63 percent also agreed, “I’ve come to accept that I have little control over what marketers can learn about me online.” Although marketers like to portray Americans as cheerfully accepting a tradeoff between their privacy and the benefits they gain, that’s [not at all](#) what’s happening. As Turow told me, “The bottom line for us is resignation. It’s not as if people want to give up their privacy, but in order to get through life they feel they have to, and they don’t feel like they have the ability to change things.”

Misconception #3: We've lost the privacy battle.

This, I would argue, is the third misconception: that the battle is lost and there's nothing people can do about protecting their privacy. It's true that there are good reasons why people feel that way — there's only so much that an individual can do to protect their privacy, especially if they're short on technical expertise or willingness to tolerate inconveniences in order to fight surveillance. It's true that our privacy depends to a large extent not on individual decisions but on collective decisions we make as a nation about the policies we want to set. It's also true that the companies that profit from surveillance are wealthy and politically powerful.

Nevertheless, the clouds are gathering for a major reckoning. The European Union has enacted a comprehensive privacy law called the General Data Protection Regulation (GDPR) that is forcing even many U.S.-centered businesses to improve their privacy practices. California, where one in eight Americans live, has also enacted a broad privacy law called the California Consumer Privacy Act (CCPA). And as these laws weaken the will of companies to oppose privacy protections, scandals such as the Cambridge Analytica fiasco have strengthened the desire of politicians across the political spectrum to support such rules. The result: For the first time in many years, members of both parties are reportedly working to draft and enact comprehensive privacy legislation.

There are major battles ahead, but, as I have argued, in the end people need — and always demand — privacy. Privacy-invading companies love it that people feel helpless, but now is the time for people to trade resignation for anger and activism, and voice that demand to ensure that any new privacy laws are strong and meaningful. The status quo is not stable, and the battle is just getting underway.



United States v. Jones: GPS Monitoring, Property, and Privacy

Richard M. Thompson II
Legislative Attorney

April 30, 2012

Congressional Research Service

7-5700

www.crs.gov

R42511

Introduction

There is little doubt that technology is fast becoming intertwined with our jobs, our social life, and even our most private interactions with each other. This phenomenon creates friction among many compelling interests. The first is a clash between two contrasting values: the desire for privacy and the longing to be connected through the newest and most advanced technology. To a certain extent, as one advances, the other must necessarily recede. Meanwhile, courts are tasked with determining the balance between government's law enforcement needs and the people's privacy. The Fourth Amendment to the U.S. Constitution provides the measuring stick to determine this balance. The amendment ensures “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.”¹ Its primary function is to prohibit government intrusion upon the privacy and property rights of the people. When new technology is involved, achieving this balance is not an easy undertaking.

United States v. Jones presented such a challenge to the Supreme Court. The question posed was whether the installation and month-long monitoring of a GPS device attached to Jones's car constituted a violation of the Fourth Amendment's prohibition against “unreasonable searches and seizures.”² This usage of the Global Positioning System (GPS)³ is not unusual in criminal investigations,⁴ but up to that point longer-term monitoring had not been directly tested by the Court. Thus, many observers awaited the *Jones* ruling for its potential impact not only on government monitoring programs, but also on general Fourth Amendment cases involving prolonged government surveillance.

In prior government tracking cases,⁵ the Court applied the test from *Katz v. United States*, which addresses whether the individual had a reasonable expectation of privacy in the area to be searched.⁶ Because the police in *Jones* physically invaded his property to attach the GPS device—whereas in the previous cases they had not—the Court declined to apply *Katz*, but instead based its decision on a trespass theory.⁷ The trespass theory asks whether there was a physical intrusion onto a constitutionally protected area coupled with an attempt to obtain information.⁸ In *Jones*, there was, so the Court applied this more limited test and held that a search occurred. Though the majority bypassed the *Katz* approach, Justice Alito, concurring with Justices Breyer, Ginsburg, and Kagan, would have applied *Katz*.⁹ Long-term surveillance, Justice

¹ U.S. Const. amend. IV.

² *United States v. Jones*, 132 S. Ct. 945, 948 (2012).

³ GPS is a network of 24 government satellites that constantly send out radio signals and allow a receiver on Earth to determine its position. Aaron Renenger, *Satellite Tracking and the Right to Privacy*, 53 HASTINGS L. J. 549, 550 (2002).

⁴ John Ganz, *It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Vehicle Tracking Devices*, 95 CRIM. L. & CRIMINOLOGY 1325, 1330 (2005).

⁵ *United States v. Knotts*, 460 U.S. 276, 278-79 (1983) (holding that use of tracking device while suspect was on public thoroughfares was not a violation of the Fourth Amendment as he had no reasonable expectation of privacy in his public movements); *United States v. Karo*, 468 U.S. 705, 718 (1984) (holding that use of tracking of device while in private home was a violation of the Fourth Amendment).

⁶ This reasonable expectation of privacy test was formulated by Justice Harlan in his *Katz* concurrence. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

⁷ *Jones*, 132 S. Ct. at 952.

⁸ *Id.* at 951 n.5.

⁹ *Id.* at 958 (Alito, J., concurring).

Alito wrote, violated Jones's reasonable expectation of privacy under *Katz*. Justice Sotomayor agreed with both the majority and Alito's concurrence, but called for additional protection by questioning the viability of the third-party doctrine, which holds that any information voluntarily given to a third party loses all privacy protections.¹⁰

This report will analyze all three opinions in an attempt to determine how *Jones* might affect future use of GPS tracking and other government surveillance techniques. First, it will briefly recount the facts that led to Jones's prosecution, his appeal, and the Supreme Court's review. Next, it will analyze the majority's property-based test, evaluating it against similar Fourth Amendment case law. Additionally, this section will raise issues concerning the possible impact of this approach on similar search and seizure cases. Next, the report will examine both Justice Alito's and Justice Sotomayor's concurrences and their potential impact on cases involving technology. Because the Court did not express whether a warrant is required, the report will posit several theories on how this issue may be resolved in the future.

United States v. Jones: A Property-Based Approach to the Fourth Amendment

In 2004, a Joint Task Force of the FBI and the District of Columbia Metropolitan Police Department suspected Antoine Jones was part of a drug distribution ring.¹¹ Based on information obtained from wiretaps, a pen register,¹² and video surveillance, the task force obtained a warrant to monitor Jones's Jeep with a GPS tracking device. According to the terms of the warrant, the officers had 10 days to install it and were required to do it in the District of Columbia. The officers installed the device on the 11th day in Maryland while the Jeep was parked in a public parking lot.¹³ For the next four weeks the device tracked Jones's every movement, creating 2,000 pages of monitoring data.¹⁴ During this time, the device tracked Jones's movements to and from a known stash house.

Jones was indicted for conspiracy to distribute and possession with intent to distribute cocaine. At trial, the prosecution relied heavily on Jones's movements derived from the GPS to connect him with a larger drug ring.¹⁵ He moved to dismiss this information as a warrantless search under the Fourth Amendment. The United States District Court for the District of Columbia excluded the data derived when his car was parked in his garage but allowed into evidence all of his public movements.¹⁶ Jones was ultimately convicted and sentenced to life imprisonment.¹⁷ The United States Court of Appeals for the District of Columbia Circuit reversed, holding that the GPS data were derived in violation of Jones's reasonable expectation of privacy under the Fourth

¹⁰ *Id.* at 957 (Sotomayor, J., concurring).

¹¹ *Id.* at 948.

¹² A pen register is a device that determines the outgoing telephone numbers dialed from a telephone. 18 U.S.C. § 3127(3).

¹³ Since the device was attached one day late and in the wrong jurisdiction, the installation was considered warrantless.

¹⁴ *Id.*

¹⁵ *Id.* at 948-49.

¹⁶ *United States v. Jones*, 451 F. Supp. 2d 71, 88 (D. D.C. 2006).

¹⁷ *Jones*, 132 S. Ct. at 949.

Amendment.¹⁸ The Supreme Court then granted a writ of certiorari, agreeing to review Jones's case.

Most observers assumed the Supreme Court would, like the D.C. Circuit Court of Appeals, apply the reasonable expectation of privacy test developed in *Katz v. United States* to determine if the tracking was a Fourth Amendment search. Under the *Katz* test, a search in the constitutional sense has occurred if the individual had an actual expectation of privacy in the area to be searched that society would deem reasonable.¹⁹ Since 1967, when *Katz* was handed down, the Court had developed a body of case law applying this privacy-based formulation of the Fourth Amendment.²⁰

The *Jones* majority, led by Justice Scalia, took a different route.²¹ It held that the *attachment* of the GPS device, coupled with its use to monitor Jones's movements, was a constitutional search.²² The Fourth Amendment ensures that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.”²³ Because Jones's vehicle is an *effect*—listed in the text of the Fourth Amendment—the police's physical intrusion by attaching the GPS for tracking purposes constituted a *search*.²⁴ This theory hinges on common law trespass as it was known in 1791 (when the Fourth Amendment was adopted). It does not rely on *Katz*, nor any subjective conception of privacy. The majority contended that Jones's rights should not strictly depend on whether his reasonably expected zone of privacy was pierced.²⁵ Rather, the majority asserted, property rights also define an individual's right to be free from government intrusion.

Justice Alito, in concurrence, contended that the majority's reliance on “18th-century tort law” which “might have provided grounds in 1791 for a suit based on trespass to chattels,” “strains the language of the Fourth Amendment; it has little if any support in current Fourth Amendment case law; and it is highly artificial.”²⁶ Justice Alito would have instead applied the *Katz* formulation.²⁷

¹⁸ *United States v. Maynard*, 615 F.3d 544, 555 (D.C. Cir. 2010). Because Jones's case was consolidated with other defendants on appeal, it was entitled *United States v. Maynard* before the D.C. Circuit Court of Appeals. It was subsequently changed back to *United States v. Jones* when reviewed by the Supreme Court.

¹⁹ *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

²⁰ See *Kyllo v. United States*, 533 U.S. 27, 32 (2001) (“In assessing when a search is not a search, we have applied somewhat in reverse the principle first enunciated in *Katz v. United States*, 389 U.S. 347, 19 L. Ed. 2d 576, 88 S. Ct. 507 (1967); *California v. Ciraolo*, 476 U.S. 207, 215 (1986) (“The touchstone of Fourth Amendment analysis is whether a person has a ‘constitutionally protected reasonable expectation of privacy.’ *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).”).

²¹ The majority consisted of Chief Justice Roberts, and Justices Thomas, Kennedy, and Sotomayor. In addition to joining the majority opinion, Justice Sotomayor also wrote a concurring opinion explored below.

²² *Jones*, 132 S. Ct. at 949.

²³ U.S. CONST. amend IV.

²⁴ *Jones*, 132 S. Ct. at 949.

²⁵ *Id.* at 950.

The Government contends that the Harlan standard shows that no search occurred here, since Jones had no “reasonable expectation of privacy” in the area of the Jeep accessed by Government agents (its underbody) and in the locations of the Jeep on the public roads, which were visible to all. But we need not address the Government's contentions, because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, we must “assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.”

Id.

²⁶ *Id.* at 958 (Alito, J., concurring).

This criticism prompts two central questions: (1) Does the majority’s property-based approach enjoy textual, historical, or jurisprudential support?; and (2) What effect will this approach have on other areas of government investigations?

The seeds for the property-based approach were planted in England in *Entick v. Carrington*, a case considered by many as an ancestor of the Fourth Amendment.²⁸ There, the English court forbade government agents from searching through Entick’s home, looking for papers intended to prove his seditious writing. The agents had a general warrant to search the home, but the warrant lacked a specific description of the area to be searched and the items to be seized. Lord Camden declared that no government agent nor any other person may enter the property of another without permission, even if no harm is done.²⁹ This theory carried over to the colonies and prompted the framers to include a prohibition against unreasonable searches and seizures when drafting the Bill of Rights.³⁰ Under this common law trespass approach, the key inquiry is not necessarily the content of the information obtained by the police, but rather their method of retrieving it. The *Jones* Court had no doubts that the attachment of the GPS device (which required a trespass of Jones’s car) would have been a search when the Fourth Amendment was adopted—when *Entick* was fresh in the framers’ minds.³¹

Although property certainly controlled Fourth Amendment thinking during the infancy of the Fourth Amendment, its control waned in later years. *Olmstead v. United States* provides an example. There, federal agents installed several wiretaps on the telephone wires coming from Olmstead’s house.³² In upholding this electronic eavesdropping, the Court ruled that the Fourth Amendment applied only when there was an official search or seizure of a person, his tangible papers and effects, and an “actual physical invasion” of the individual’s home.³³ Because the installation of the wiretap did not require the agents to trespass onto Olmstead’s property, the Court held that it was not a search or seizure under the Fourth Amendment.³⁴

Forty years later, the Court began its shift away from this property-centric approach. In *Warden v. Hayden*, the Court noted the property-based approach had been discredited over the years, and that privacy should be the focus of the inquiry under the Fourth Amendment.³⁵ Subsequently, the Court decided *Katz v. United States*, where it held an electronic surveillance of Katz’s conversations while he was in a public telephone booth was impermissible, despite the fact that no property rights were involved.³⁶ The “Fourth Amendment protects people, not places,” the

(...continued)

²⁷ *Id.*

²⁸ *Entick v. Carrington*, 95 Eng. Rep. 807 (C.P. 1765); see Ricardo J. Bascaus, *Property and Probable Cause: The Fourth Amendment’s Principled Protection of Privacy*, 60 RUTGERS L. REV. 575, 581-82 (2008).

²⁹ *Entick v. Carrington*, 95 Eng. Rep. 807 (C.P. 1765).

³⁰ See Amil Akir, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 767 (1994).

³¹ *Jones*, 132 S. Ct. at 950.

³² *Olmstead v. United States*, 277 U.S. 438, 456-57 (1928).

³³ *Id.* at 466.

³⁴ *Id.*

³⁵ *Warden, Maryland Penitentiary v. Hayden*, 387 U.S. 294, 304 (1967) (“We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts.”).

³⁶ *Katz v. United States*, 389 U.S. 347, 359 (1967).

Court declared, and any search that invaded a person’s “reasonable expectation of privacy”³⁷ should be considered a search in the constitutional sense.

This seemingly conflicting line of cases left many wondering whether property and privacy could coexist under the Fourth Amendment. The Court attempted to reconcile these two lines in *Soldal v. County of Cook*.³⁸ There, while under the supervision of local police, a landlord had his tenant’s trailer home towed from the rented lot.³⁹ The tenant sued the police under Section 1983, a civil rights statute, for a violation of his Fourth Amendment right to be free from unreasonable seizure. The Seventh Circuit Court of Appeals denied the tenant’s claim, holding that any Fourth Amendment violation must be supported by some invasion of privacy.⁴⁰ The police did not invade the tenant’s privacy, but only his possessory interest in the property, enough for the court to hold the Fourth Amendment inapplicable. Instead, the panel noted that the due process clause was the proper avenue of relief for a “pure deprivation of property.”⁴¹

The Supreme Court disagreed, ruling that the police action was a seizure notwithstanding the lack of a privacy interest at stake.⁴² The Court took pains to note that privacy-based cases like *Katz* and *Warden* had not “snuffed out the previously recognized protection for property under the Fourth Amendment,” but instead had “demonstrated that property is not the sole measure of Fourth Amendment violations.”⁴³ The Court noted that the amendment does not protect possessory interests in all kinds of property, such as an open field not closely connected with a person’s home, but certainly covers things specifically listed in the constitutional text—persons, houses, papers, and effects.⁴⁴

This idea that the Fourth Amendment protects both privacy and property independently is infused throughout the majority opinion in *Jones*. As Justice Scalia noted, *Katz* did not *supplant* the common law trespass approach, but merely *supplemented* it.⁴⁵ But is a simple trespass alone enough to constitute a violation? The Court answered no: in addition to the physical intrusion, there must be “an attempt to find something or to obtain information.”⁴⁶ Also, not every police trespass will be a constitutional search. The government must intrude upon an area enumerated in the text of the amendment (person, houses, papers, and effects).⁴⁷ This leaves several questions. If a car is an effect, what other personal property may be covered under this approach? Will computer data constitute an *effect*? Will an e-mail constitute an electronic *paper*? If a police

³⁷ *Id.* at 351, 360 (Harlan, J., concurring).

³⁸ *Soldal v. County of Cook*, 506 U.S. 56 (1992).

³⁹ *Id.* at 58.

⁴⁰ *Soldal v. County of Cook*, 942 F.2d 1073, 1078 (7th Cir. 1991).

⁴¹ *Id.*

⁴² *Soldal*, 506 U.S. at 65.

⁴³ *Id.* at 64.

⁴⁴ *Id.* at 64 n.7.

⁴⁵ *Jones*, 132 S. Ct. at 950-951.

⁴⁶ *Id.* at 951 n.5. It is not clear from the majority opinion whether a mere attempt to obtain information is enough, or if the attempt must be successful. In one phrasing the Court requires “installation of a GPS device on a target’s vehicle, and its *use* of that device....,” *Id.* at 949 (emphasis added), and in another it requires a trespass plus “an *attempt* to find or to obtain information.” *Id.* at 951 n.5 (emphasis added). A reasonable interpretation is that an attempt is enough: if the police were to come into a person’s home looking for evidence, but found nothing, this would probably qualify under the majority’s approach.

⁴⁷ *Id.* at 953 n.8.

officer walks onto one's porch, is that an invasion of his *house*? There are no easy answers to these questions.

Additionally, because the Court focused on the attachment of the device and the property interests involved, there remain questions of whether prolonged tracking with a device is permissible under the Fourth Amendment if there is no trespass. As the majority noted, “[s]ituations involving merely transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.”⁴⁸ Justice Alito’s and Sotomayor’s concurrences in *Jones* may be scrutinized for how the Court might handle these scenarios under *Katz*.⁴⁹

The Implications of *Jones* and Technology

As more cell phones and cars are outfitted with GPS tracking technologies, police need not physically attach a device to track its movements. Because the *Jones* majority opinion is based on a *physical* trespass into a constitutionally protected area, it seemingly will not apply where GPS is preinstalled. Justices Alito, and his four-Justice concurrence, and Sotomayor, concurring separately, provide insight into how a future court may apply the Fourth Amendment to evolving technologies.⁵⁰ These opinions rely, to a certain extent, on the mosaic theory first discussed in the D.C. Circuit opinion, which says that tracking a person’s public movements over a long duration is constitutionally unacceptable even if tracking each of the movements individually may be permitted. Whether this approach will garner a majority on the Court is unclear. However, at a minimum, these concurrences have engendered discussion in the lower courts, with several courts citing the mosaic theory as a viable alternative.⁵¹

The question then becomes how much weight should the Alito and Sotomayor concurring opinions be accorded?⁵² There is no *one* rule to answer this question.⁵³ Generally, there are two types of concurrences in Supreme Court opinions. The first is the true concurrence, in which the Justice concurs in the judgment, but disagrees with the reasoning.⁵⁴ Justice Alito’s opinion exemplifies that type of concurrence; he agreed that the surveillance constituted a Fourth

⁴⁸ *Id.* at 953.

⁴⁹ The importance of these concurrences was noted by an FBI attorney: “[E]ven though its not technically holding, we have to anticipate how it’s going to go down the road.” Julia Angwin, *FBI Turns Off Thousands of GPS Devices After Supreme Court Ruling* (Feb. 25, 2012, 3:36 PM), <http://blogs.wsj.com/digits/2012/02/25/fbi-turns-off-thousands-of-gps-devices-after-supreme-court>.

⁵⁰ *Jones*, 132 S. Ct. at 854 (Sotomayor, J., concurring); 132 S. Ct. at 957 (Alito, J., concurring).

⁵¹ *United States v. Hanna*, No. 11-20678-CR, 2012 WL 279435, at *3 (S.D. Fla. Jan. 3, 2012) (analyzing the issue of Fourth Amendment standing under both the trespass theory and *Katz*’s privacy test); *United States v. Bradshaw*, No. 1:11-CR-257, 2012 WL 774964 (N.D. Ohio Mar. 8, 2012) (noting that the *Jones* majority did not adopt the mosaic theory); *State v. Zahn*, No. 25584, 2012 WL 862707 (S.D. Mar. 14, 2012) (holding that both the trespass approach and the mosaic theory can apply to GPS tracking).

⁵² This dialogue between concurring justices and those they are trying to persuade lies at the heart of the common law system—a case-by-case discussion between judges, lawyers, and the public about the progression of the law. RICHARD A. POSNER, THE FEDERAL COURTS: CRISIS AND REFORM 236 (1985).

⁵³ Igor Kirman, *Standing Apart to Be a Part: The Precedential Value of Supreme Court Concurring Opinions*, 95 COLUM L. REV. 2083, 2096-2101 (1995) (explaining that some courts will presume precedential value in a concurring opinion while others will presume no precedential value).

⁵⁴ Lewis A. Kornhauser & Lawrence G. Sager, *The One and the Many: Adjudication in Collegial Courts*, 81 CAL. L. REV. 1 (1993).

Amendment search, but would have decided the case under the traditional reasonable expectation of privacy test instead of the trespass test. The second category is the simple concurrence, where the Justice agrees with the judgment and the reasoning of the majority,⁵⁵ but also poses possible new theories that may not be directly relevant to that particular case, but can be used later to move the law in a particular direction.⁵⁶ Justice Sotomayor's opinion seems to fit this latter category. Although these two concurrences chart somewhat different courses in their strategy and reasoning, when combined they appear to command five votes on the Court—a potential majority.⁵⁷

Justice Alito's Concurrence: A *Katz*-Based Approach

Justice Alito spends most of his concurrence attempting to counter the majority's common law trespass theory.⁵⁸ He argued that Scalia's reversion to the law as it stood in 1791 was unwise, and a return to the much-criticized property approach.⁵⁹ The focus of this report, however, is Justice Alito's discussion of long-term GPS tracking under *Katz*'s reasonable expectation of privacy test.

Before coming up on appeal, the D.C. Circuit below examined whether Jones's whereabouts over the month-long period of tracking were *exposed* to the public.⁶⁰ A person's movements are not *actually* exposed, the court answered, because the likelihood that anyone could actually follow someone for a month is highly improbable.⁶¹ Further, the movements are not *constructively* exposed because in many instances the whole is greater than the sum of the parts.⁶² This last proposition is premised on the mosaic theory. The mosaic theory supposes that tracking the whole of one's movements over an extended period of time reveals significantly more about that person than each individual trip does in isolation.⁶³ For instance, police cannot infer much about a person from *one* trip to the liquor store. However, a *daily* trip to the same liquor store would provide greater insight into the person's habits. The government has employed this theory in the national security context for protecting intelligence sources and methods of obtaining information.⁶⁴ The thrust of the argument is that unless a person has a broad view of the situation in question, he will not understand the importance of a single piece of evidence.⁶⁵ Thus, with GPS tracking, following someone for one trip may not say much about a person, but following his every movement for an extended period presumably reveals considerably more.

⁵⁵ Kirman, *supra* note 53, 2119.

⁵⁶ Scott C. Idleman, *A Prudential Theory of Judicial Candor*, 73 TEX. L. REV. 1307, 1371 (1995).

⁵⁷ Mark Tushnet, *Themes in Warren Court Biographies*, 70 N.Y.U. L. REV. 748, 763 (1995).

⁵⁸ *Jones*, 132 S. Ct. at 957 (Alito, J., concurring) Justice Alito contended that the Court melded the two distinct acts of *search* and *seizure* into one to develop its holding; that this approach is merely a return to the much-criticized *Olmstead*, when property controlled; that there are no 18th century analogs to GPS; and that the attachment would not suffice even under common tort law. *Id.*

⁵⁹ *Jones*, 132 S. Ct. at 958-59 (Alito, J., concurring).

⁶⁰ United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010).

⁶¹ *Id.* at 558.

⁶² *Id.*

⁶³ *Id.* at 561-62.

⁶⁴ Cen. Int. Agency v. Sims, 471 U.S. 159, 178 (1985).

⁶⁵ *Id.* at 178.

United States v. Knotts created an obstacle to the panel's adoption of the mosaic theory.⁶⁶ In *Knotts*, the Supreme Court held that a person has no reasonable expectation of privacy in his movements on public streets.⁶⁷ The Court, however, did not foreclose the argument that, even if traveling on public roadways, pervasive or intrusive police activity may violate the Fourth Amendment.⁶⁸ The Court suggested it would revisit the issue if police were to use "dragnet-type law enforcement practices."⁶⁹ Although the purport of this phrase is somewhat obscure, the D.C. Circuit understood it to mean that 24-hour surveillance of a single individual was sufficient for it to apply.⁷⁰ As such, the panel ruled that the previous tracking cases were not controlling, allowing it to apply the mosaic theory.⁷¹ Based on this application, the court granted Jones's motion to dismiss all location evidence obtained from the GPS device.

As noted earlier, Justice Scalia and the majority did not apply the mosaic theory. Instead they grounded their decision in a common law trespass theory.⁷² Justice Alito, on the other hand, wanted to confront directly this question of how technology affected a society's expectations of privacy. He first posited that the ubiquity of cell phones, video monitoring, and other technologies in modern life shapes the average person's expectation of privacy—presumably reducing that expectation.⁷³ Based on his understanding of *Katz*, Alito would have asked whether the use of GPS tracking involved an intrusion a reasonable person would not have expected. Under his approach, "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable."⁷⁴ However, the use of "longer term" GPS monitoring will in most instances violate the Fourth Amendment.⁷⁵ Justice Alito declined to create a rule for determining at what point police tracking crosses this constitutional line. He concluded that four weeks of tracking was a search.⁷⁶

Because of the limited nature of Justice Alito's discussion, it is difficult to discern precisely which theory he employed. It is arguable that he and the three other Justices implicitly support the mosaic theory. To say that short-term monitoring is permissible, but longer-term monitoring is not, indicates there is something about the aggregation of a person's movements that prompted these Justices to deem it a Fourth Amendment search.⁷⁷ It could also be argued that Justice Alito's

⁶⁶ *United States v. Knotts*, 460 U.S. 276, 281 (1983).

⁶⁷ *Knotts*, 460 U.S. at 281.

⁶⁸ *Id.* at 283.

⁶⁹ *Id.* This phrase was dicta, meaning it was not essential to the case; thus it is persuasive, but not binding on lower courts.

⁷⁰ *Maynard*, 615 F.3d at 556.

⁷¹ *Id.* at 558.

⁷² *Jones*, 132 S. Ct. at 951. The Court did not repudiate the mosaic theory, but instead did not reach the question of whether this privacy-based theory would apply; the property-based approach was sufficient to resolve the case.

⁷³ *Id.* at 958 (Alito, J., concurring). Query whether the reasonable expectation of privacy test is designed to test what privacy the average person would expect. See Orin Kerr, *The Fourth Amendment and New Technologies*, 102 MICH. L. REV. 801, 838 (2004) ("A 'reasonable expectation of privacy' has not been equated with the expectation of privacy of a reasonable person; rather, it has been used as a term of art based heavily on property law principles.").

⁷⁴ *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

⁷⁵ *Id.*

⁷⁶ *Id.*

⁷⁷ The mosaic theory need not be cabined to only the GPS tracking scenario. It could apply in other contexts such as smart electric meters, Internet searches, or any other activity in which surveillance of activity over a long period of time can be aggregated to produce an in-depth look into the subject's daily activities, belief systems, etc. CRS Report R42338, *Smart Meter Data: Privacy and Cybersecurity*, by Brandon J. Murrill, Edward C. Liu, and Richard M. (continued...)

concurrence did not accept the mosaic theory, but instead applied the probabilistic model of Fourth Amendment theory.⁷⁸ This theory supposes that when government conducts an investigation in a way that would surprise an individual, or “interferes with customs and social expectations,” it violates a reasonable expectation of privacy.⁷⁹ Justice Alito categorizes the *Katz* test as looking at the “privacy expectations of the hypothetical reasonable person”—a hypothetical person who has “a well-developed and stable set of privacy expectations.”⁸⁰ Justice Alito notes that in precomputer days, the police had the time and resources to track only persons of exceptional interest to the police. He seems to accord much importance in the belief that the hypothetical reasonable person would be surprised to learn that the police would be tracking their every movement for a month-long period—an act beyond society’s expectations.

Justice Sotomayor’s Concurrence: The Broadest Reading of the Fourth Amendment

As far as Fourth Amendment rights are concerned, Justice Sotomayor provided the broadest interpretation in *Jones* by joining the majority’s trespass approach, openly supporting Justice Alito’s privacy-based approach,⁸¹ and putting into question the continuing viability of the third-party doctrine—a theory many believe creates the largest gap in privacy protection, especially in the realm of technology.

Whereas it is unclear whether Justices Alito, Breyer, Kagan, and Ginsburg support the mosaic theory, Justice Sotomayor maintained that this theory should directly guide the Court’s determination of a person’s privacy expectations in their public movements.⁸² She noted that “GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.”⁸³ As part and parcel of the mosaic theory, she contended that an individual’s awareness that the government may be constantly watching can chill one’s freedom of speech and association under the First Amendment.⁸⁴ Although the police might obtain the same evidence through traditional surveillance, there is something about the technology that troubled Justice Sotomayor. She seemed concerned that there will no longer be a logistical barrier between the government and the people. Police now have access to a cheap technology that can produce a significant amount of data. The Court must consider this a search—presumably requiring a warrant—to provide adequate oversight over the executive branch.⁸⁵ This idea seems to coincide with Justice Jackson’s well-worn saying that courts prefer that searches be overseen by a “neutral

(...continued)

Thompson II.

⁷⁸ Orin Kerr, *What’s the Status of the Mosaic Theory After Jones?*, THE VOLOKH CONSPIRACY (Jan. 23, 2012, 1:59 PM), <http://volokh.com/2012/01/23/whats-the-status-of-the-mosaic-theory-after-jones/>.

⁷⁹ Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 509 (2007).

⁸⁰ *Jones*, 132 S. Ct. at 962 (Alito, J., concurring).

⁸¹ Although she could not join his opinion, Justice Sotomayor clearly supported Justice Alito’s reasoning. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (“As Justice Alito incisively observes”; “I agree with Justice Alito....”).

⁸² *Id.*

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ *Id.*

and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.”⁸⁶

Additionally, Justice Sotomayor called for a reexamination of the third-party doctrine. This doctrine supposes that any information a person voluntarily conveys to a third party is no longer entitled to Fourth Amendment protection, as the person cannot have a reasonable expectation that the third party will guard the privacy in that information.⁸⁷ This rule has been used to justify access to bank records,⁸⁸ the telephone numbers a person dials,⁸⁹ electric billing records,⁹⁰ and cell phone billing records.⁹¹ Some argue that when individuals give documents to a third party, usually in a commercial transaction, they consent to the release of such information to the government,⁹² or at a minimum assume the risk that the person trusted with the information would hand it over.⁹³ Justice Sotomayor suggests that perhaps this theory should not be permitted to reach its logical extent in the digital age, in which people convey a wealth of personal information to third parties.⁹⁴ She contends that the Fourth Amendment rules should not require a person to keep secret any information the person does not want the government to obtain. In the end, she leaves it to another day to reevaluate the third-party doctrine in an age where most private information is handed over in the course of commercial transactions. In the meantime, Justice Sotomayor believed the physical intrusion theory was enough to resolve the case.⁹⁵

⁸⁶ *Johnson v. United States*, 333 U.S. 10, 14 (1948).

⁸⁷ *United States v. Miller*, 425 U.S. 435, 443 (1976). “The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”

Id.

⁸⁸ *Miller*, 425 U.S. at 435.

⁸⁹ *Smith v. Maryland*, 442 U.S. 735 (1979).

⁹⁰ *United States v. McIntyre*, 646 F.3d 1107 (8th Cir. 2011).

⁹¹ *United States v. Hynson*, No. 05-576, 2007 WL 2692327, at *6 (E.D. Pa. Sept. 11, 2007).

⁹² See Orin S. Kerr, *The Case for a Third-Party Doctrine*, 107 MICH. L. REV. 561, 565 (2009).

⁹³ *Smith*, 442 U.S. at 744 (“Because the depositor [in *Miller*] ‘assumed the risk’ of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private.”).

⁹⁴ *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

⁹⁵ *Id.*

JUDITH JARVIS THOMSON

The Right to Privacy

I

Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is. Consider, for example, the familiar proposal that the right to privacy is the right "to be let alone." On the one hand, this doesn't seem to take in enough. The police might say, "We grant we used a special X-ray device on Smith, so as to be able to watch him through the walls of his house; we grant we trained an amplifying device on him so as to be able to hear everything he said; but we let him strictly alone: we didn't touch him, we didn't even go near him—our devices operate at a distance." Anyone who believes there is a right to privacy would presumably believe that it has been violated in Smith's case; yet he would be hard put to explain precisely how, if the right to privacy is the right to be let alone. And on the other hand, this account of the right to privacy lets in far too much. If I hit Jones on the head with a brick I have not let him alone. Yet, while hitting Jones on the head with a brick is surely violating some right of Jones', doing it should surely not turn out to violate his right to privacy. Else, where is this to end? Is *every* violation of a right a violation of the right to privacy?

It seems best to be less ambitious, to begin with at least. I suggest,

I am grateful to the members of the Society for Ethical and Legal Philosophy for criticisms of the first draft of the following paper. Alan Sparer made helpful criticisms of a later draft.

then, that we look at some specific, imaginary cases in which people would say, "There, in that case, the right to privacy has been violated," and ask ourselves precisely why this would be said, and what, if anything, would justify saying it.

II

But there is a difficulty to be taken note of first. What I have in mind is that there may not be so much agreement on the cases as I implied. Suppose that my husband and I are having a fight, shouting at each other as loud as we can; and suppose that we have not thought to close the windows, so that we can easily be heard from the street outside. It seems to me that anyone who stops to listen violates no right of ours; stopping to listen is at worst bad, Not Nice, not done by the best people. But now suppose, by contrast, that we are having a quiet fight, behind closed windows, and cannot be heard by the normal person who passes by; and suppose that someone across the street trains an amplifier on our house, by means of which he can hear what we say; and suppose that he does this in order to hear what we say. It seems to me that anyone who does this does violate a right of ours, the right to privacy, I should have thought.

But there is room for disagreement. It might be said that in neither case is there a violation of a right, that both are cases of mere bad behavior—though no doubt worse behavior in the second case than in the first, it being very much naughtier to train amplifiers on people's houses than merely to stop in the street to listen.

Or, alternatively, it might be said that in both cases there is a violation of a right, the right to privacy in fact, but that the violation is less serious in the first case than in the second.

I think that these would both be wrong. I think that we have in these two cases, not merely a difference in degree, but a difference in quality: that the passerby who stops to listen in the first case may act badly, but violates no one's rights, whereas the neighbor who uses an amplifier in the second case does not merely act badly but violates a right, the right to privacy. But I have no argument for this. I take it rather as a datum in this sense: it seems to me there would be a mark against an account of the right to privacy if it did not yield the

conclusion that these two cases do differ in the way I say they do, and moreover explain why they do.

But there is one thing perhaps worth drawing attention to here: doing so may perhaps diminish the inclination to think that a right is violated in both cases. What I mean is this. There is a familiar account of rights—I speak now of rights generally, and not just of the right to privacy—according to which a man's having a right that something shall not be done to him just itself consists in its being the case that anyone who does it to him acts badly or wrongly or does what he ought not do. Thus, for example, it is said that to have a right that you shall not be killed or imprisoned just itself consists in its being the case that if anyone does kill or imprison you, he acts badly, wrongly, does what he ought not do. If this account of rights were correct, then my husband and I would have a right that nobody shall stop in the street and listen to our loud fight, since anyone who does stop in the street and listen acts badly, wrongly, does what he ought not do. Just as we have a right that people shall not train amplifiers on the house to listen to our quiet fights.

But this account of rights is just plain wrong. There are many, many things we ought not do to people, things such that if we do them to a person, we act badly, but which are not such that to do them is to violate a right of his. It is bad behavior, for example to be ungenerous and unkind. Suppose that you dearly love chocolate ice cream but that, for my part, I find that a little of it goes a long way. I have been given some and have eaten a little, enough really, since I don't care for it very much. You then, looking on, ask, "May I have the rest of your ice cream?" It would be bad indeed if I were to reply, "No, I've decided to bury the rest of it in the garden." I ought not do that; I ought to give it to you. But you have no right that I give it to you, and I violate no right of yours if I do bury the stuff.

Indeed, it is possible that an act which is not a violation of a right should be a far worse act than an act which is. If you did not merely want that ice cream but needed it, for your health perhaps, then my burying it would be monstrous, indecent, though still, of course, no violation of a right. By contrast, if you snatch it away, steal it, before I can bury it, then while you violate a right (the ice cream is mine,

after all), your act is neither monstrous nor indecent—if it's bad at all, it's anyway not very bad.

From the point of view of conduct, of course, this doesn't really matter: bad behavior is bad behavior, whether it is a violation of a right or not. But if we want to be clear about *why* this or that bit of bad behavior is bad, then these distinctions do have to get made and looked into.

III

To return, then, to the two cases I drew attention to, and which I suggest we take to differ in this way: in one of them a right is violated, in the other not. It isn't, I think, the fact that an amplifying device is used in the one case, and not in the other, that is responsible for this difference. On the one hand, consider someone who is deaf: if he passes by while my husband and I are having a loud fight at an open window and turns up his hearing-aid so as to be able to hear us, it seems to me he no more violates our right to privacy than does one who stops to listen and can hear well enough without a hearing-aid. And on the other hand, suppose that you and I have to talk over some personal matters. It is most convenient to meet in the park, and we do so, taking a bench far from the path since we don't want to be overheard. It strikes a man to want to know what we are saying to each other in that heated fashion, so he creeps around in the bushes behind us and crouches back of the bench to listen. He thereby violates the right to privacy—fully as much as if he had stayed a hundred yards away and used an amplifying device to listen to us.

IV

The cases I drew attention to are actually rather difficult to deal with, and I suggest we back away from them for a while and look at something simpler.

Consider a man who owns a pornographic picture. He wants that nobody but him shall ever see that picture—perhaps because he wants that nobody shall know that he owns it, perhaps because he feels that someone else's seeing it would drain it of power to please. So he keeps it locked in his wall-safe, and takes it out to look at only at night or after pulling down the shades and closing the curtains. We have

heard about his picture, and we want to see it, so we train our X-ray device on the wall-safe and look in. To do this is, I think, to violate a right of his—the right to privacy, I should think.

No doubt people who worry about violations of the right to privacy are not worried about the possibility that others will look at their possessions. At any rate, this doesn't worry them very much. That it is not nothing, however, comes out when one thinks on the special source of discomfort there is if a burglar doesn't go straight for the TV set and the silver, and then leave, but if he stops for a while just to look at things—e.g. at your love letters or at the mound of torn socks on the floor of your closet. The trespass and the theft *might* swamp everything else; but they might not: the burglar's merely looking around in that way might make the episode feel worse than it otherwise would have done.

So I shall suppose that we do violate this man's right to privacy if we use an X-ray device to look at the picture in his wall-safe. And now let us ask how and why.

To own a picture is to have a cluster of rights in respect of it. The cluster includes, for example, the right to sell it to whomever you like, the right to give it away, the right to tear it, the right to look at it. These rights are all "positive rights": rights to do certain things to or in respect of the picture. To own a picture is also to have certain "negative rights" in respect of it, that is, rights that others shall not do certain things to it—thus, for example, the right that others shall not sell it or give it away or tear it.

Does owning a picture also include having the negative right that others shall not look at it? I think it does. If our man's picture is good pornography, it would be pretty mingy of him to keep it permanently hidden so that nobody but him shall ever see it—a nicer person would let his friends have a look at it too. But he is within his rights to hide it. If someone is about to tear his picture, he can snatch it away: it's his, so he has a right that nobody but him shall tear it. If someone is about to look at his picture, he can snatch it away or cover it up: it's his, so he has a right that nobody but him shall look at it.

It is important to stress that he has not merely the right to snatch the picture away in order that nobody shall tear it, he has not merely

the right to do everything he can (within limits) to prevent people from tearing it, he has also the right that nobody *shall* tear it. What I have in mind is this. Suppose we desperately want to tear his picture. He locks it in his wall-safe to prevent us from doing so. And suppose we are so eager that we buy a penetrating long-distance picture-tearer: we sit quietly in our apartment across the street, train the device on the picture in the wall-safe, press the button—and lo! we have torn the picture. The fact that he couldn't protect his picture against the action of the device doesn't make it all right that we use it.

Again, suppose that there was a way in which he could have protected his picture against the action of the device: the rays won't pass through platinum, and he could have encased the picture in platinum. But he would have had to sell everything else he owns in order to pay for the platinum. The fact he didn't do this does not make it all right for us to have used the device.

We all have a right to do what we can (within limits) to secure our belongings against theft. I gather, however, that it's practically impossible to secure them against a determined burglar. Perhaps only hiring armed guards or sealing the house in solid steel will guarantee that our possessions cannot be stolen; and perhaps even these things won't work. The fact (if it's a fact) that we can't guarantee our belongings against theft; the fact (if it's a fact) that though we can, the cost of doing so is wildly out of proportion to the value of the things, and therefore we don't; neither of these makes it all right for the determined burglar to walk off with them.

Now I said that if a man owns a picture he can snatch it away or he can cover it up to prevent anyone else from *looking* at it. He can also hide it in his wall-safe. But I think he has a right, not merely to do what he can (within limits) to prevent it from being looked at: he has a right that it shall not be looked at—just as he has a right that it shall not be torn or taken away from him. That he has a right that it shall not be looked at comes out, I think, in this way: if he hides it in his wall-safe, and we train our X-ray device on the wall-safe and look in, we have violated a right of his in respect of it, and the right is surely the right that it shall not be looked at. The fact that he couldn't protect his picture against the action of an X-ray device which enables us to look at it doesn't make it all right that we use the X-ray

device to look at it—just as the fact that he can't protect his picture against the action of a long-distance picture-tearing device which enables us to tear his picture doesn't make it all right that we use the device to tear it.

Compare, by contrast, a subway map. You have no right to take it off the wall or cover it up: you haven't a right to do whatever you can to prevent it from being looked at. And if you do cover it up, and if anyone looks through the covering with an X-ray device, he violates no right of yours: you do not have a right that nobody but you shall look at it—it's not *yours*, after all.

Looking at a picture doesn't harm it, of course, whereas tearing a picture does. But this doesn't matter. If I use your toothbrush I don't harm it; but you, all the same, have a right that I shall not use it.

However, to have a right isn't always to claim it. Thus, on any view to own a picture is to have (among other rights) the right that others shall not tear it. Yet you might want someone else to do this and therefore (1) invite him to, or (2) get him to whether he wants to or not—e.g. by carefully placing it where he'll put his foot through it when he gets out of bed in the morning. Or again, while not positively wanting anyone else to tear the picture, you might not care whether or not it is torn, and therefore you might simply (3) let someone tear it—e.g. when, out of laziness, you leave it where it fell amongst the things the children are in process of wrecking. Or again still, you might positively want that nobody shall tear the picture and yet in a fit of absent-mindedness (4) leave it in some place such that another person would have to go to some trouble if he is to avoid tearing it, or (5) leave it in some place such that another person could not reasonably be expected to know that it still belonged to anybody.

Similarly, you might want someone else to look at your picture and therefore (1) invite him to, or (2) get him to whether he wants to or not. Or again, while not positively wanting anyone else to look at the picture, you might not care whether or not it is looked at, and therefore you might simply (3) let it be looked at. Or again still, you might positively want that nobody shall look at the picture, and yet in a fit of absent-mindedness (4) leave it in some place such that another person would have to go to some trouble if he is to avoid looking at it (at least, avert his eyes) or (5) leave it in some place

such that another person could not reasonably be expected to know that it still belonged to anybody.

In all of these cases, it is permissible for another person on the one hand to tear the picture, on the other to look at it: no right of the owner's is violated. I think it fair to describe them as cases in which, though the owner had a right that the things not be done, he *waived* the right: in cases (1), (2), and (3) intentionally, in cases (4) and (5) unintentionally. It is not at all easy to say under what conditions a man has waived a right—by what acts of commission or omission and in what circumstances. The conditions vary, according as the right is more or less important; and while custom and convention, on the one hand, and the cost of securing the right, on the other hand, play very important roles, it is not clear precisely what roles. Nevertheless there plainly is such a thing as waiving a right; and given a man has waived his right to a thing, we violate no right of his if we do not accord it to him.

There are other things which may bring about that although a man had a right to a thing, we violate no right of his if we do not accord it to him: he may have transferred the right to another or he may have forfeited the right or he may still have the right, though it is overridden by some other, more stringent right. (This is not meant to be an exhaustive list.) And there are also some circumstances in which it is not clear what should be said. Suppose someone steals your picture and invites some third party (who doesn't know it's yours) to tear it or look at it; or suppose someone takes your picture by mistake, thinking it's his, and invites some third party (who doesn't know it's yours) to tear it or look at it; does the *third* party violate a right of yours if he accepts the invitation? A general theory of rights should provide an account of all of these things.

It suffices here, however, to stress one thing about rights: a man may have had a right that we shall not do a thing, he may even still have a right that we shall not do it, consistently with its being the case that we violate no right of his if we go ahead.

If this is correct, we are on the way to what we want. I said earlier that when we trained our X-ray device on that man's wall-safe in order to have a look at his pornographic picture, we violated a right

of his, the right to privacy, in fact. It now turns out (if I am right) that we violated a property right of his, specifically the negative right that others shall not look at the picture, this being one of the (many) rights which his owning the picture consists of. I shall come back a little later to the way in which these rights interconnect.

V

We do not, of course, care nearly as much about our possessions as we care about ourselves. We do not want people looking at our torn socks; but it would be much worse to have people watch us make faces at ourselves in the mirror when we thought no one was looking or listen to us while we fight with our families. So you might think I have spent far too much time on that pornographic picture.

But in fact, if what I said about pornographic pictures was correct, then the point about ourselves comes through easily enough. For if we have fairly stringent rights over our property, we have very much more stringent rights over our own persons. None of you came to possess your knee in exactly the way in which you came to possess your shoes or your pornographic pictures: I take it you neither bought nor inherited your left knee. And I suppose you could not very well sell your left knee. But that isn't because it isn't yours to sell—some women used to sell their hair, and some people nowadays sell their blood—but only because who'd buy a used left knee? For if anyone wanted to, you are the only one with a right to sell yours. Again, it's a nasty business to damage a knee; but you've a right to damage yours, and certainly nobody else has—its being your left knee includes your having the right that nobody else but you shall damage it. And, as I think, it also includes your having the right that nobody else shall touch it or look at it. Of course you might invite somebody to touch or look at your left knee; or you might let someone touch or look at it; or again still, you might in a fit of absent-mindedness leave it in some place such that another person would have to go to some trouble if he is to avoid touching or looking at it. In short, you might waive your right that your left knee not be touched or looked at. But that is what doing these things would be: waiving a right.

I suppose there are people who would be deeply distressed to learn

that they had absent-mindedly left a knee uncovered, and that somebody was looking at it. Fewer people would be deeply distressed to learn that they had absent-mindedly left their faces uncovered. Most of us wouldn't, but Moslem women would; and so might a man whose face had been badly disfigured, in a fire, say. Suppose you woke up one morning and found that you had grown fangs or that you no longer had a nose; you might well want to claim a right which most of us so contentedly waive: the right that your face not be looked at. That we have such a right comes out when we notice that if a man comes for some reason or another to want his face not to be looked at, and if he therefore keeps it covered, and if we then use an X-ray device in order to be able to look at it through the covering, we violate a right of his in respect of it, and the right we violate is surely the right that his face shall not be looked at. Compare again, by contrast, a subway map. No matter how much you may want a subway map to not be looked at, if we use an X-ray device in order to be able to look at it through the covering you place over it, we violate no right of yours: you do not have a right that nobody but you shall look at it—it is not *yours*, after all.

Listening, I think, works in the same way as looking. Suppose you are an opera singer, a great one, so that lots of people want to listen to you. You might sell them the right to listen. Or you might invite them to listen or let them listen or absent-mindedly sing where they cannot help but listen. But if you have decided you are no longer willing to be listened to; if you now sing only quietly, behind closed windows and carefully sound-proofed walls; and if somebody trains an amplifier on your house so as to be able to listen, he violates a right, the right to not be listened to.

These rights—the right to not be looked at and the right to not be listened to¹—are analogous to rights we have over our property. It

1. In "A Definition of Privacy," *Rutgers Law Review*, 1974, p. 281, Richard B. Parker writes:

The definition of privacy defended in this article is that *privacy is control over when and by whom the various parts of us can be sensed by others*. By "sensed," is meant simply seen, heard, touched, smelled, or tasted. By "parts of us," is meant the parts of our bodies, our voices, and the products of our bodies. "Parts of us" also includes objects very closely associated with us. By "closely associated" is meant primarily what is spatially associated. The ob-

sounds funny to say we have such rights. They are not mentioned when we give lists of rights. When we talk of rights, those that come to mind are the grand ones: the right to life, the right to liberty, the right to not be hurt or harmed, and property rights. Looking at and listening to a man do not harm him, but neither does stroking his left knee harm him, and yet he has a right that it shall not be stroked without permission. Cutting off all a man's hair while he's asleep will not harm him, nor will painting his elbows green; yet he plainly has a right that these things too shall not be done to him. These un-grand rights seem to be closely enough akin to be worth grouping together under one heading. For lack of a better term, I shall simply speak of "the right over the person," a right which I shall take to consist of the un-grand rights I mentioned, and others as well.

When I began, I said that if my husband and I are having a quiet fight behind closed windows and cannot be heard by the normal person who passes by, then if anyone trains an amplifier on us in order to listen he violates a right, the right to privacy, in fact. It now turns out (if I am right) that he violates our right to not be listened to, which is one of the rights included in the right over the person.

I had said earlier that if we use an X-ray device to look at the pornographic picture in a man's wall-safe, we violate his right to privacy. And it then turned out (if I was right) that we violated the

jects which are "parts of us" are objects we usually keep with us or locked up in a place accessible only to us.

The right to privacy, then, is presumably the right to this control. But I find this puzzling, on a number of counts. First, why *control*? If my neighbor invents an X-ray device which enables him to look through walls, then I should imagine I thereby lose control over who can look at me: going home and closing the doors no longer suffices to prevent others from doing so. But my right to privacy is not violated until my neighbor actually does train the device on the wall of my house. It is the actual looking that violates it, not the acquisition of power to look. Second, there are other cases. Suppose a more efficient bugging device is invented: instead of tapes, it produces neatly typed transcripts (thereby eliminating the middlemen). One who reads those transcripts does not *hear* you, but your right to privacy is violated just as if he does.

On the other hand, this article is the first I have seen which may be taken to imply (correctly, as I think) that there are such rights as the right to not be looked at and the right to not be listened to. And in any case, Professor Parker's interest is legal rather than moral: he is concerned to find a definition which will be useful in legal contexts. (I am incompetent to estimate how successful he is in doing this.)

I am grateful to Charles Fried for drawing my attention to this article.

right that others shall not look at the picture, which is one of the rights which his owning the picture consists in.

It begins to suggest itself, then, as a simplifying hypothesis, that the right to privacy is itself a cluster of rights, and that it is not a distinct cluster of rights but itself intersects with the cluster of rights which the right over the person consists in and also with the cluster of rights which owning property consists in. That is, to use an X-ray device to look at the picture is to violate a right (the right that others shall not look at the picture) which is both one of the rights which the right to privacy consists in and also one of the rights which property-ownership consists in. Again, that to use an amplifying device to listen to us is to violate a right (the right to not be listened to) which is both one of the rights which the right to privacy consists in and also one of the rights which the right over the person consists in.

Some small confirmation for this hypothesis comes from the other listening case. I had said that if my husband and I are having a loud fight, behind open windows, so that we can easily be heard by the normal person who passes by, then if a passerby stops to listen, he violates no right of ours, and so in particular does not violate our right to privacy. Why doesn't he? I think it is because, though he listens to us, we have *let him listen* (whether intentionally or not), we have waived our right to not be listened to—for we took none of the conventional and easily available steps (such as closing the windows and lowering our voices) to prevent listening. But this would only be an explanation if waiving the right to not be listened to were waiving the right to privacy, or if it were at least waiving the only one among the rights which the right to privacy consists in which might plausibly be taken to have been violated by the passerby.

But for further confirmation, we shall have to examine some further violations of the right to privacy.

VI

The following cases are similar to the ones we have just been looking at.
(a) A deaf spy trains on your house a bugging device which produces, not sounds on tape, but a typed transcript, which he then reads. (Cf. footnote 1.) (b) A blind spy trains on your house an X-ray device

which produces, not views of you, but a series of bas-relief panels, which he then feels. The deaf spy doesn't listen to you, the blind spy doesn't look at you, but both violate your right to privacy just as if they did.

It seems to me that in both these cases there is a violation of that same right over the person which is violated by looking at or listening to a person. You have a right, not merely that you not be looked at or listened to but also that you not have your words transcribed, and that you not be modeled in bas-relief. These are rights that the spies violate, and it is these rights in virtue of the violation of which they violate your right to privacy. Of course, one may waive these rights: a teacher presumably waives the former when he enters the classroom, and a model waives the latter when he enters the studio. So these cases seem to present no new problem.

VII

A great many cases turn up in connection with information.

I should say straightaway that it seems to me none of us has a right over any fact to the effect that that fact shall not be known by others. You may violate a man's right to privacy by looking at him or listening to him; there is no such thing as violating a man's right to privacy by simply knowing something about him.

Where our rights in this area do lie is, I think, here: we have a right that certain steps shall not be taken to find out facts, and we have a right that certain uses shall not be made of facts. I shall briefly say a word about each of these.

If we use an X-ray device to look at a man in order to get personal information about him, then we violate his right to privacy. Indeed, we violate his right to privacy whether the information we want is personal or impersonal. We might be spying on him in order to find out what he does all alone in his kitchen at midnight; or we might be spying on him in order to find out how to make puff pastry, which we already know he does in the kitchen all alone at midnight; either way his right to privacy is violated. But in both cases, the simplifying hypothesis seems to hold: in both cases we violate a right (the right to not be looked at) which is both one of the rights which the right

to privacy consists in and one of the rights which the right over the person consists in.

What about torturing a man in order to get information? I suppose that if we torture a man in order to find out how to make puff pastry, then though we violate his right to not be hurt or harmed, we do not violate his right to privacy. But what if we torture him to find out what he does in the kitchen all alone at midnight? Presumably in that case we violate both his right to not be hurt or harmed and his right to privacy—the latter, presumably, because it was personal information we tortured him to get. But here too we can maintain the simplifying hypothesis: we can take it that to torture a man in order to find out personal information is to violate a right (the right to not be tortured to get personal information) which is both one of the rights which the right to privacy consists in and one of the rights which the right to not be hurt or harmed consists in.

And so also for extorting information by threat: if the information is not personal, we violate only the victim's right to not be coerced by threat; if it is personal, we presumably also violate his right to privacy—in that we violate his right to not be coerced by threat to give personal information, which is both one of the rights which the right to privacy consists in and one of the rights which the right to not be coerced by threat consists in.

I think it a plausible idea, in fact, that doing something to a man to get personal information from him is violating his right to privacy only if doing that to him is violating some right of his not identical with or included in the right to privacy. Thus writing a man a letter asking him where he was born is no violation of his right to privacy: writing a man a letter is no violation of any right of his. By contrast, spying on a man to get personal information is a violation of the right to privacy, and spying on a man for any reason is a violation of the right over the person, which is not identical with or included in (though it overlaps) the right to privacy. Again, torturing a man to get personal information is presumably a violation of the right to privacy, and torturing a man for any reason is a violation of the right to not be hurt or harmed, which is not identical with or included in (though it overlaps) the right to privacy. If the idea is right, the sim-

plifying hypothesis is trivially true for this range of cases. If a man has a right that we shall not do such and such to him, then he has a right that we shall not do it to him in order to get personal information from him. And his right that we shall not do it to him in order to get personal information from him is included in both his right that we shall not do it to him, and (if doing it to him for this reason is violating his right to privacy) his right to privacy.

I suspect the situation is the same in respect of uses of information. If a man gives us information on the condition we shall not spread it, and we then spread it, we violate his right to confidentiality, whether the information is personal or impersonal. If the information is personal, I suppose we also violate his right to privacy—by virtue of violating a right (the right to confidentiality in respect of personal information) which is both one of the rights which the right to privacy consists in and one of the rights which the right to confidentiality consists in. The point holds whether our motive for spreading the information is malice or profit or anything else.

Again, suppose I find out by entirely legitimate means (e.g. from a third party who breaks no confidence in telling me) that you keep a pornographic picture in your wall-safe; and suppose that, though I know it will cause you distress, I print the information in a box on the front page of my newspaper, thinking it newsworthy: Professor Jones of State U. Keeps Pornographic Picture in Wall-Safe! Do I violate your right to privacy? I am, myself, inclined to think not. But if anyone thinks I do, he can still have the simplifying hypothesis: he need only take a stand on our having a right that others shall not cause us distress, and then add that what is violated here is the right to not be caused distress by the publication of personal information, which is one of the rights which the right to privacy consists in, and one of the rights which the right to not be caused distress consists in. Distress, after all, is the heart of the wrong (if there is a wrong in such a case): a man who positively wants personal information about himself printed in newspapers, and therefore makes plain he wants it printed, is plainly not wronged when newspapers cater to his want.

(My reluctance to go along with this is not due to a feeling that we have no such right as the right to not be caused distress: that we have

such a right seems to me a plausible idea. So far as I can see, there is nothing special about physical hurts and harms; mental hurts and harms are hurts and harms too. Indeed, they may be more grave and long-lasting than the physical ones, and it is hard to see why we should be thought to have rights against the one and not against the other. My objection is, rather, that even if there is a right to not be caused distress by the publication of personal information, it is mostly, if not always, overridden by what seems to me a more stringent right, namely the public's right to a press which prints any and all information, personal or impersonal, which it deems newsworthy; and thus that in the case I mentioned no right is violated, and hence, a fortiori, the right to privacy is not violated.²

VIII

The question arises, then, whether or not there are *any* rights in the right to privacy cluster which aren't also in some other right cluster. I suspect there aren't any, and that the right to privacy is everywhere overlapped by other rights. But it's a difficult question. Part of the difficulty is due to its being (to put the best face on it) unclear just what is in this right to privacy cluster. I mentioned at the outset that there is disagreement on cases; and the disagreement becomes even more stark as we move away from the kinds of cases I've so far been drawing attention to which seem to me to be the central, core cases.

What should be said, for example, of the following?

(a) The neighbors make a terrible racket every night. Or they cook foul-smelling stews. Do they violate my right to privacy? Some think yes, I think not. But even if they do violate my right to privacy, perhaps all would be well for the simplifying hypothesis since their doing this is presumably a violation of another right of mine, roughly, the right to be free of annoyance in my house.

(b) The city, after a city-wide referendum favoring it, installs

2. It was Warren and Brandeis, in their now classic article, "The Right to Privacy," *Harvard Law Review*, 1890, who first argued that the law ought to recognize wrongs that are (they thought) committed in cases such as these. For a superb discussion of this article, see Harry Kalven, Jr., "Privacy in Tort Law—Were Warren and Brandeis Wrong?" *Law and Contemporary Problems*, Spring 1966.

loudspeakers to play music in all the buses and subways. Do they violate my right to privacy? Some think yes, I think not. But again perhaps all is well: it is if those of us in the minority have a right to be free of what we (though not the majority) regard as an annoyance in public places.

(c) You are famous, and photographers follow you around, everywhere you go, taking pictures of you. Crowds collect and stare at you. Do they violate your right to privacy? Some think yes, I think not: it seems to me that if you do go out in public, you waive your right to not be photographed and looked at. But of course you, like the rest of us, have a right to be free of (what anyone would grant was) annoyance in public places; so in particular, you have a right that the photographers and crowds not press in too closely.

(d) A stranger stops you on the street and asks, "How much do you weigh?" Or an acquaintance, who has heard of the tragedy, says, "How terrible you must have felt when your child was run over by that delivery truck!"³ Or a cab driver turns around and announces, "My wife is having an affair with my psychoanalyst." Some think that your right to privacy is violated here; I think not. There is an element of coercion in such cases: the speaker is trying to force you into a relationship you do not want, the threat being your own embarrassment at having been impolite if you refuse. But I find it hard to see how we can be thought to have a right against such attempts. Of course the attempt may be an annoyance. Or a sustained series of such attempts may become an annoyance. (Consider, for example, an acquaintance who takes to stopping at your office *every morning* to ask if you slept well.) If so, I suppose a right *is* violated, namely, the right against annoyances.

(e) Some acquaintances of yours indulge in some very personal gossip about you.⁴ Let us imagine that all of the information they share was arrived at without violation of any right of yours, and that none of the participants violates a confidence in telling what he tells. Do they violate a right of yours in sharing the information? If they do, there is trouble for the simplifying hypothesis, for it seems to me there is no right not identical with, or included in, the right to privacy

3. Example from Thomas Nagel.

4. Example from Gilbert Harman.

cluster which they could be thought to violate. On the other hand, it seems to me they *don't* violate any right of yours. It seems to me we simply do not have rights against others that they shall not gossip about us.

(f) A state legislature makes it illegal to use contraceptives. Do they violate the right to privacy of the citizens of that state? No doubt certain techniques for enforcing the statute (e.g., peering into bedroom windows) would be obvious violations of the right to privacy; but is there a violation of the right to privacy in the mere enacting of the statute—in addition to the violations which may be involved in enforcing it? I think not. But it doesn't matter for the simplifying hypothesis if it is: making a kind of conduct illegal is infringing on a liberty, and we all of us have a right that our liberties not be infringed in the absence of compelling need to do so.

IX

The fact, supposing it a fact, that every right in the right to privacy cluster is also in some other right cluster does not by itself show that the right to privacy is in any plausible sense a "derivative" right. A more important point seems to me to be this: the fact that we have a right to privacy does not explain our having any of the rights in the right to privacy cluster. What I have in mind is this. We have a right to not be tortured. Why? Because we have a right to not be hurt or harmed. I have a right that my pornographic picture shall not be torn. Why? Because it's mine, because I own it. I have a right to do a somersault now. Why? Because I have a right to liberty. I have a right to try to preserve my life. Why? Because I have a right to life. In these cases we explain the having of one right by appeal to the having of another which includes it. But I don't have a right to not be looked at because I have a right to privacy; I don't have a right that no one shall torture me in order to get personal information about me because I have a right to privacy; one is inclined, rather, to say that it is because I have *these* rights that I have a right to privacy.

This point, supposing it correct, connects with what I mentioned at the outset: that nobody seems to have any very clear idea what the right to privacy is. We are confronted with a cluster of rights—a cluster

with disputed boundaries—such that most people think that to violate at least any of the rights in the core of the cluster is to violate the right to privacy; but what have they in common other than their being rights such that to violate them is to violate the right to privacy? To violate these rights is to not let someone alone? To violate these rights is to visit indignity on someone? There are too many acts in the course of which we do not let someone alone, in the course of which we give affront to dignity, but in the performing of which we do not violate anyone's right to privacy. That we feel the need to find something in common to all of the rights in the cluster and, moreover, feel we haven't yet got it in the very fact that they *are* all in the cluster, is a consequence of our feeling that one cannot explain our having any of the rights in the cluster in the words: "Because we have a right to privacy."

But then if, as I take it, every right in the right to privacy cluster is also in some other right cluster, there is no need to find the that-which-is-in-common to all rights in the right to privacy cluster and no need to settle disputes about its boundaries. For if I am right, the right to privacy is "derivative" in this sense: it is possible to explain in the case of each right in the cluster how come we have it without ever once mentioning the right to privacy. Indeed, the wrongness of every violation of the right to privacy can be explained without ever once mentioning it. Someone tortures you to get personal information from you? He violates your right to not be tortured to get personal information from you, and you have that right because you have the right to not be hurt or harmed—and it is because you have this right that what he does is wrong. Someone looks at your pornographic picture in your wall-safe? He violates your right that your belongings not be looked at, and you have that right because you have ownership rights—and it is because you have them that what he does is wrong. Someone uses an X-ray device to look at you through the walls of your house? He violates your right to not be looked at, and you have that right because you have rights over your person analogous to the rights you have over your property—and it is because you have these rights that what he does is wrong.

In any case, I suggest it is a useful heuristic device in the case of

any purported violation of the right to privacy to ask whether or not the act is a violation of any other right, and if not whether the act *really* violates a right at all. We are still in such deep dark in respect of rights that any simplification at all would be well worth having.⁵

5. Frederick Davis' article, "What Do We Mean by 'Right to Privacy'?" *South Dakota Law Review*, Spring 1959, concludes, in respect of tort law, that

If truly fundamental interests are accorded the protection they deserve, no need to champion a right to privacy arises. Invasion of privacy is, in reality, a complex of more fundamental wrongs. Similarly, the individual's interest in privacy itself, however real, is derivative and a state better vouchsafed by protecting more immediate rights [p. 20]. . . . Indeed, one can logically argue that the concept of a right to privacy was never required in the first place, and that its whole history is an illustration of how well-meaning but impatient academicians can upset the normal development of the law by pushing it too hard [p. 230].

I am incompetent to assess this article's claims about the law, but I take the liberty of warmly recommending it to philosophers who have an interest in looking further into the status and nature of the right to privacy.

How TikTok is supporting our community through COVID-19

Legal

If you are a user having your usual residence in the US, this [Privacy Policy](#) shall apply.

If you are a user having your usual residence in the EEA, United Kingdom or Switzerland, this [Privacy Policy](#) shall apply.

If you are not in the US, EEA, United Kingdom or Switzerland, this [Privacy Policy](#) shall apply. There may also be jurisdiction specific provisions for certain countries or regions. Please refer to your local privacy policy for more information.

Privacy Policy

(If you are a user having your usual residence in the US)

Last updated: December 20, 2020.

Welcome to TikTok (the “Platform”). The Platform is provided and controlled by TikTok Inc. (“TikTok”, “we” or “us”). We are committed to protecting and respecting your privacy. This Privacy Policy covers the experience we provide for users age 13 and over on our Platform. For information about our under-13 experience (“Children’s Platform”) and our practices in the United States regarding children’s privacy, please refer to our [Privacy Policy for Younger Users](#).

Capitalized terms that are not defined in this policy have the meaning given to them in the [Terms of Service](#).

What information do we collect?

We collect information when you create an account and use the Platform. We also collect information you share with us from third-party social network providers, and technical and behavioral information about your use of the Platform. We also collect information contained in the messages you send through our Platform and information from your phone book, if you grant us access to your phone book on your mobile device. More information about the categories and sources of information is provided below.

Information you choose to provide

For certain activities, such as when you register, upload content to the Platform, or contact us directly, you may provide some or all of the following information:

- Registration information, such as age, username and password, language, and email or phone number
- Profile information, such as name, social media account information, and profile image
- User-generated content, including comments, photographs, videos, and virtual item videos that you choose to upload or broadcast on the Platform (“User Content”)
- Payment information, such as PayPal or other third-party payment information (where required for the purpose of payment)
- Your phone and social network contacts, with your permission. If you choose to find other users through your phone contacts, we will access and collect the names and phone numbers and match that information against existing users of the Platform. If you choose to find other users through your social network contacts, we will collect your public profile information as well as names and profiles of your social contacts
- Your opt-in choices and communication preferences
- Information to verify an account
- Information in correspondence you send to us
- Information you share through surveys or your participation in challenges, sweepstakes, or contests such as your gender, age, likeness, and preferences.

Information we obtain from other sources

We may receive the information described in this Privacy Policy from other sources, such as:

Social Media. If you choose to link or sign up using your social network (such as Facebook, Twitter, Instagram, or Google), we may collect information from these social media services, including your contact lists for these services and information relating to your use of the Platform in relation to these services.

Third-Party Services. We may collect information about you from third-party services, such as advertising partners and analytics providers.

Others Users of the Platform. Sometimes other users of the Platform may provide us information about you, including through customer service inquiries.

Other Sources. We may collect information about you from other publicly available sources.

Information we collect automatically

We automatically collect certain information from you when you use the Platform, including internet or other network activity information such as your IP address, geolocation-related data (as described

below), unique device identifiers, browsing and search history (including content you have viewed in the Platform), and Cookies (as defined below).

Usage Information

We collect information regarding your use of the Platform and any other User Content that you generate through and broadcast on our Platform. We also link your subscriber information with your activity on our Platform across all your devices using your email, phone number, or similar information.

Device Information

We collect information about the device you use to access the Platform, including your IP address, unique device identifiers, model of your device, your mobile carrier, time zone setting, screen resolution, operating system, app and file names and types, keystroke patterns or rhythms, and platform.

Location data

We collect information about your location, including location information based on your SIM card and/or IP address. With your permission, we may also collect Global Positioning System (GPS) data.

Messages

We collect and process, which includes scanning and analyzing, information you provide in the context of composing, sending, or receiving message through the Platform's messaging functionality. That information includes the content of the message and information about when the message has been sent, received and/or read, as well as the participants of the communication. Please be aware that messages sent to other users of the Platform will be accessible by those users and that we are not responsible for the manner in which those users use or disclose messages.

Metadata

When you upload User Content, you automatically upload certain metadata that is connected to the User Content. Metadata describes other data and provides information about your User Content that will not always be evident to the viewer. In connection with your User Content the metadata can describe how, when, and by whom the piece of User Content was collected and how that content is formatted. It also includes information, such as your account name, that enables other users to trace back the User Content to your user account. Additionally, metadata will consist of data that you chose to provide with your User Content, e.g. any hashtags used to mark keywords to the video and captions.

Cookies

We and our service providers and business partners use cookies and other similar technologies (e.g. web beacons, flash cookies, etc.) (“Cookies”) to automatically collect information, measure and analyze which web pages you click on and how you use the Platform, enhance your experience using the Platform, improve the Platform, and provide you with targeted advertising on the Platform and elsewhere across your different devices. Cookies are small files which, when placed on your device, enable the Platform to provide certain features and functionality. Web beacons are very small images or small pieces of data embedded in images, also known as “pixel tags” or “clear GIFs,” that can recognize Cookies, the time and date a page is viewed, a description of the page where the pixel tag is placed, and similar information from your computer or device. To learn how to disable Cookies, see your “Your choices” section below.

Additionally, we allow these service providers and business partners to collect information about your online activities through Cookies. We and our service providers and business partners link your contact or subscriber information with your activity on our Platform across all your devices, using your email or other log-in or device information. Our service providers and business partners may use this information to display advertisements on our Platform and elsewhere online and across your devices tailored to your interests, preferences, and characteristics. We are not responsible for the privacy practices of these service providers and business partners, and the information practices of these service providers and business partners are not covered by this Privacy Policy.

We may aggregate or de-identify the information described above. Aggregated or de-identified data is not subject to this Privacy Policy.

How we use your information

As explained below, we use your information to fulfill and enforce our Terms of Service, to improve and administer the Platform, and to allow you to use its functionalities. We may also use your information to, among other things, show you suggestions, promote the Platform, and customize your ad experience.

We generally use the information we collect:

- To fulfill requests for products, services, Platform functionality, support and information for internal operations, including troubleshooting, data analysis, testing, research, statistical, and survey purposes and to solicit your feedback
- To customize the content you see when you use the Platform. For example, we may provide you with services based on the country settings you have chosen or show you content that is similar to content that you like or interacted with
- To send promotional materials from us or on behalf of our affiliates and trusted third parties
- To improve and develop our Platform and conduct product development

- To measure and understand the effectiveness of the advertising we serve to you and others and to deliver targeted advertising
- To make suggestions and provide a customized ad experience
- To support the social functions of the Platform, including to permit you and other users to connect with each other through the Platform and for you and other users to share, download, and otherwise interact with User Content posted through the Platform
- To use User Content as part of our advertising and marketing campaigns to promote the Platform
- To understand how you use the Platform, including across your devices
- To infer additional information about you, such as your age, gender, and interests
- To help us detect abuse, fraud, and illegal activity on the Platform
- To ensure that you are old enough to use the Platform (as required by law)
- To communicate with you, including to notify you about changes in our services
- To announce you as a winner of our contest, sweepstakes, or promotions if permitted by the promotion rule, and to send you any applicable prizes
- To enforce our terms, conditions, and policies
- Consistent with your permissions, to provide you with location-based services, such as advertising and other personalized content
- To inform our algorithms
- To combine all the information we collect or receive about you for any of the foregoing purposes
- For any other purposes disclosed to you at the time we collect your information or pursuant to your consent.

How we share your information

We are committed to maintaining your trust, and while TikTok does not sell personal information to third parties, we want you to understand when and with whom we may share the information we collect for business purposes.

Service Providers and Business Partners

We share the categories of personal information listed above with service providers and business partners to help us perform business operations and for business purposes, including research,

payment processing and transaction fulfillment, database maintenance, administering contests and special offers, technology services, deliveries, email deployment, advertising, analytics, measurement, data storage and hosting, disaster recovery, search engine optimization, marketing, and data processing. These service providers and business partners may include:

- Payment processors and transaction fulfillment providers, who may receive the information you choose to provide, the information we obtain from other sources, and the information we collect automatically but who do not receive your message data.
- Customer and technical support providers, who may receive the information you choose to provide, the information we obtain from other sources, and the information we collect automatically.
- Researchers, who may receive the information you choose to provide, the information we obtain from other sources, and the information we collect automatically but would not receive your payment information or message data.
- Cloud providers, who may receive the information you choose to provide, the information we obtain from other sources, and the information we collect automatically.
- Advertising, marketing, and analytics vendors, who may receive the information you choose to provide, the information we obtain from other sources, and the information we collect automatically but would not receive your payment information or message data.

Within Our Corporate Group

We may share all of the information we collect with a parent, subsidiary, or other affiliate of our corporate group.

In Connection with a Sale, Merger, or Other Business Transfer

We may share all of the information we collect in connection with a substantial corporate transaction, such as the sale of a website, a merger, consolidation, asset sales, or in the unlikely event of bankruptcy.

For Legal Reasons

We may disclose any of the information we collect to respond to subpoenas, court orders, legal process, law enforcement requests, legal claims, or government inquiries, and to protect and defend the rights, interests, safety, and security to TikTok Inc., the Platform, our affiliates, users, or the public. We may also share any of the information we collect to enforce any terms applicable to the Platform, to exercise or defend any legal claims, and comply with any applicable law.

With Your Consent

We may share your information for other purposes pursuant to your consent or with your further direction.

If you access third-party services, such as Facebook, Google, or Twitter, to login to the Platform or to share information about your usage on the Platform with others, these third-party services may be able to collect information about you, including information about your activity on the Platform, and they may notify your connections on the third-party services about your use of the Platform, in accordance with their privacy policies.

If you choose to engage in public activities on the Platform, you should be aware that any information you share may be read, collected, or used by other users. You should use caution in disclosing personal information while engaging. We are not responsible for the information you choose to submit.

Your Rights

You may submit a request to access or delete the information we have collected about you by sending your request to us at the email or physical address provided in the Contact section at the bottom of this policy. You may be entitled, in accordance with applicable law, to submit a request through an authorized agent. To designate an authorized agent to exercise choices on your behalf, please provide evidence that you have given such agent power of attorney or that the agent otherwise has valid written authority to submit requests to exercise rights on your behalf. We will respond to your request consistent with applicable law and subject to proper verification. We will verify your request by asking you to send it from the email address associated with your account or to provide information necessary to verify your account. And we do not discriminate based on the exercise of any privacy rights that you might have.

Your Choices

- You may be able to refuse or disable Cookies by adjusting your browser settings. Because each browser is different, please consult the instructions provided by your browser. Please note that you may need to take additional steps to refuse or disable certain types of Cookies. For example, due to differences in how browsers and mobile apps function, you may need to take different steps to disable Cookies used for targeted advertising in a browser and to disable targeted advertising for a mobile application, which you may control through your device settings or mobile app permissions. In addition, our choice to disable cookies is specific to the particular browser or device that you are using when you disable cookies, so you may need to separately disable cookies for each type of browser or device. If you choose to refuse, disable, or delete Cookies, some of the functionality of the Platform may no longer be available to you. Without this information, we are not able to provide you with all the requested services, and any differences in services are related to your information.

- You can manage third-party advertising preferences for some of the third parties we work with to serve advertising across the Internet by clicking here and by utilizing the choices available at www.networkadvertising.org/managing/opt_our.asp and www.aboutads.info/choices.
- Your mobile device may include a feature that allows you to opt out of some types of targeted advertising (“Limit Ad Tracking” on iOS and “Opt out of Interest-Based Ads” on Android).
- You can opt out of marketing or advertising emails by utilizing the “unsubscribe” link or mechanism noted in marketing or advertising emails.
- You can switch off GPS location information functionality on your mobile device if you do not wish to share GPS information.
- If you have registered for an account you may access, review, and update certain personal information that you have provided to us by logging into your account and using available features and functionalities.
- Some browsers transmit “do-not-track” signals to websites. Because of differences in how browsers incorporate and activate this feature, it is not always clear whether users intend for these signals to be transmitted, or whether they even are aware of them. We currently do not take action in response to these signals.

Security

We use reasonable measures to help protect information from loss, theft, misuse and unauthorized access, disclosure, alteration, and destruction. You should understand that no data storage system or transmission of data over the Internet or any other public network can be guaranteed to be 100 percent secure. Please note that information collected by third parties may not have the same security protections as information you submit to us, and we are not responsible for protecting the security of such information.

Children

The privacy of users under the age of 13 (“Younger Users”) is important to us. We provide a separate experience for Younger Users in the United States on the Children’s Platform, in which we collect only limited information. For more information on our United States data collection practices for Younger Users, please visit the [Privacy Policy for Younger Users](#).

The Platform otherwise is not directed at children under the age of 13. If we become aware that personal information has been collected on the Platform from a person under the age of 13 we will delete this information and terminate the person’s account. If you believe that we have collected information from a child under the age of 13 on the Platform, contact us at: <https://tiktok.com/legal/report/privacy>.

Other Rights

Sharing for Direct Marketing Purposes (Shine the Light)

If you are a California resident, once a calendar year, you may be entitled to obtain information about personal information that we shared, if any, with other businesses for their own direct marketing uses. If applicable, this information would include the categories of customer information, as well as the names and addresses of those businesses with which we shared customer information for the immediately prior calendar year. To submit a request, contact us at:

<https://www.tiktok.com/legal/report/privacy>.

Content Removal for Users Under 18

Users of the Platform who are California residents and are under 18 years of age may request and obtain removal of User Content they posted by contacting us at:

<https://www.tiktok.com/legal/report/privacy>. All requests must be labeled “California Removal Request” on the email subject line. All requests must provide a description of the user Content you want removed and information reasonably sufficient to permit us to locate that User Content. We do not accept California Removal Requests via postal mail, telephone, or facsimile. We are not responsible for notices that are not labeled or sent properly, and we may not be able to respond if you do not provide adequate information. Please note that your request does not ensure complete or comprehensive removal of the material. For example, materials that you have posted may be republished or reposted by another user or third party.

Changes

We may update this Privacy Policy from time to time. When we update the Privacy Policy, we will notify you by updating the “Last Updated” date at the top of this policy and posting the new Privacy Policy and providing any other notice required by applicable law. We recommend that you review the Privacy Policy each time you visit the Platform to stay informed of our privacy practices.

Contact

Questions, comments and requests regarding this policy should be addressed to:

- Mailing Address: TikTok Inc., Attn: TikTok Legal Department 10100 Venice Blvd, Suite 401, Culver City, CA 90232, USA
- Contact us: <https://www.tiktok.com/legal/report/privacy>

HARVARD LAW REVIEW.

VOL. IV.

DECEMBER 15, 1890.

NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in *Millar v. Taylor*, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession — intangible, as well as tangible.

Thus, with the recognition of the legal value of sensations, the protection against actual bodily injury was extended to prohibit mere attempts to do such injury; that is, the putting another in

fear of such injury. From the action of battery grew that of assault.¹ Much later there came a qualified protection of the individual against offensive noises and odors, against dust and smoke, and excessive vibration. The law of nuisance was developed.² So regard for human emotions soon extended the scope of personal immunity beyond the body of the individual. His reputation, the standing among his fellow-men, was considered, and the law of slander and libel arose.³ Man's family relations became a part of the legal conception of his life, and the alienation of a wife's affections was held remediable.⁴ Occasionally the law halted,—as in its refusal to recognize the intrusion by seduction upon the honor of the family. But even here the demands of society were met. A mean fiction, the action *per quod servitium amisit*, was resorted to, and by allowing damages for injury to the parents' feelings, an adequate remedy was ordinarily afforded.⁵ Similar to the expansion of the right to life was the growth of the legal conception of property. From corporeal property arose the incorporeal rights issuing out of it; and then there opened the wide realm of intangible property, in the products and processes of the mind,⁶

¹ Year Book, Lib. Ass., folio 99, pl. 60 (1348 or 1349), appears to be the first reported case where damages were recovered for a civil assault.

² These nuisances are technically injuries to property; but the recognition of the right to have property free from interference by such nuisances involves also a recognition of the value of human sensations.

³ Year Book, Lib. Ass., folio 177, pl. 19 (1356), (2 Finl. Reeves Eng. Law, 395) seems to be the earliest reported case of an action for slander.

⁴ Winsmore *v.* Greenbank, Willes, 577 (1745).

⁵ Loss of service is the gist of the action; but it has been said that "we are not aware of any reported case brought by a parent where the value of such services was held to be the measure of damages." Cassoday, J., in Lavery *v.* Crooke, 52 Wis. 612, 623 (1881). First the fiction of constructive service was invented; Martin *v.* Payne, 9 John. 387 (1812). Then the feelings of the parent, the dishonor to himself and his family, were accepted as the most important element of damage. Bedford *v.* McKowl, 3 Esp. 119 (1800); Andrews *v.* Askey, 8 C. & P. 7 (1837); Phillips *v.* Hoyle, 4 Gray, 568 (1855); Phelin *v.* Kenderdine, 20 Pa. St. 354 (1853). The allowance of these damages would seem to be a recognition that the invasion upon the honor of the family is an injury to the parent's person, for ordinarily mere injury to parental feelings is not an element of damage, *e.g.*, the suffering of the parent in case of physical injury to the child. Flemington *v.* Smithers, 2 C. & P. 292 (1827); Black *v.* Carrollton R. R. Co., 10 La. Ann. 33 (1855); Covington Street Ry. Co. *v.* Packer, 9 Bush, 455 (1872).

⁶ "The notion of Mr. Justice Yates that nothing is property which cannot be earmarked and recovered in detinue or trover, may be true in an early stage of society, when property is in its simple form, and the remedies for violation of it also simple, but is not true in a more civilized state, when the relations of life and the interests arising therefrom are complicated." Erle, J., in Jefferys *v.* Boosey, 4 H. L. C. 815, 869 (1854).

as works of literature and art,¹ goodwill,² trade secrets, and trademarks.³

This development of the law was inevitable. The intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature.

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone."⁴ Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons;⁵ and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer.⁶ The alleged facts of a somewhat notorious case brought before an inferior tribunal in New York a few months ago,⁷ directly involved the consideration

¹ Copyright appears to have been first recognized as a species of private property in England in 1558. *Drone on Copyright*, 54, 61.

² *Gibblett v. Read*, 9 Mod. 459 (1743), is probably the first recognition of goodwill as property.

³ *Hogg v. Kirby*, 8 Ves. 215 (1803). As late as 1742 Lord Hardwicke refused to treat a trade-mark as property for infringement upon which an injunction could be granted. *Blanchard v. Hill*, 2 Atk. 484.

⁴ *Cooley on Torts*, 2d ed., p. 29.

⁵ 8 Amer. Law Reg. N. S. 1 (1869); 12 Wash. Law Rep. 353 (1884); 24 Sol. J. & Rep. 4 (1879).

⁶ *Scribner's Magazine*, July, 1890. "The Rights of the Citizen: To his Reputation," by E. L. Godkin, Esq., pp. 65, 67.

⁷ *Marion Manola v. Stevens & Myers*, N. Y. Supreme Court, "New York Times" of June 15, 18, 21, 1890. There the complainant alleged that while she was playing in the Broadway Theatre, in a rôle which required her appearance in tights, she was, by means of a flash light, photographed surreptitiously and without her consent, from one of the boxes by defendant Stevens, the manager of the "Castle in the Air" company, and defendant Myers, a photographer, and prayed that the defendants might be restrained from making use of the photograph taken. A preliminary injunction issued *ex parte*, and a time was set for argument of the motion that the injunction should be made permanent, but no one then appeared in opposition.

of the right of circulating portraits ; and the question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration.

Of the desirability — indeed of the necessity — of some such protection, there can, it is believed, be no doubt. The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle. The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual ; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. Nor is the harm wrought by such invasions confined to the suffering of those who may be made the subjects of journalistic or other enterprise. In this, as in other branches of commerce, the supply creates the demand. Each crop of unseemly gossip, thus harvested, becomes the seed of more, and, in direct proportion to its circulation, results in a lowering of social standards and of morality. Even gossip apparently harmless, when widely and persistently circulated, is potent for evil. It both belittles and perverts. It belittles by inverting the relative importance of things, thus dwarfing the thoughts and aspirations of a people. When personal gossip attains the dignity of print, and crowds the space available for matters of real interest to the community, what wonder that the ignorant and thoughtless mistake its relative importance. Easy of comprehension, appealing to that weak side of human nature which is never wholly cast down by the misfortunes and frailties of our neighbors, no one can be surprised that it usurps the place of interest in brains capable of other things. Triviality destroys at once robustness of thought and delicacy of feeling. No enthusiasm can flourish, no generous impulse can survive under its blighting influence.

It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual ; and, if it does, what the nature and extent of such protection is.

Owing to the nature of the instruments by which privacy is invaded, the injury inflicted bears a superficial resemblance to the wrongs dealt with by the law of slander and of libel, while a legal remedy for such injury seems to involve the treatment of mere wounded feelings, as a substantive cause of action. The principle on which the law of defamation rests, covers, however, a radically different class of effects from those for which attention is now asked. It deals only with damage to reputation, with the injury done to the individual in his external relations to the community, by lowering him in the estimation of his fellows. The matter published of him, however widely circulated, and however unsuited to publicity, must, in order to be actionable, have a direct tendency to injure him in his intercourse with others, and even if in writing or in print, must subject him to the hatred, ridicule, or contempt of his fellow-men, — the effect of the publication upon his estimate of himself and upon his own feelings not forming an essential element in the cause of action. In short, the wrongs and correlative rights recognized by the law of slander and libel are in their nature material rather than spiritual. That branch of the law simply extends the protection surrounding physical property to certain of the conditions necessary or helpful to worldly prosperity. On the other hand, our law recognizes no principle upon which compensation can be granted for mere injury to the feelings. However painful the mental effects upon another of an act, though purely wanton or even malicious, yet if the act itself is otherwise lawful, the suffering inflicted is *damnum absque injuria*. Injury of feelings may indeed be taken account of in ascertaining the amount of damages when attending what is recognized as a legal injury ;¹

¹ Though the legal value of "feelings" is now generally recognized, distinctions have been drawn between the several classes of cases in which compensation may or may not be recovered. Thus, the fright occasioned by an assault constitutes a cause of action, but fright occasioned by negligence does not. So fright coupled with bodily injury affords a foundation for enhanced damages ; but, ordinarily, fright unattended by bodily injury cannot be relied upon as an element of damages, even where a valid cause of action exists, as in trespass *quare clausum frig. t.* *Wvman v. Leavitt*, 71 Me. 227; *Canning v. Williamstown*, 1 *Cush.* 451. The allowance of damages for injury to the parents'

but our system, unlike the Roman law, does not afford a remedy even for mental suffering which results from mere contumely and insult, from an intentional and unwarranted violation of the "honor" of another.¹

It is not however necessary, in order to sustain the view that the common law recognizes and upholds a principle applicable to cases of invasion of privacy, to invoke the analogy, which is but superficial, to injuries sustained, either by an attack upon reputation or by what the civilians called a violation of honor; for the legal doctrines relating to infractions of what is ordinarily termed the common-law right to intellectual and artistic property are, it is believed, but instances and applications of a general right to privacy, which properly understood afford a remedy for the evils under consideration.

The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.² Under our system of government, he can never be compelled to express them (except when upon the witness-stand); and even if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them. The existence of this right does not depend upon the particular

feelings, in case of seduction, abduction of a child (*Stowe v. Heywood*, 7 All. 118), or removal of the corpse of child from a burial-ground (*Meagher v. Driscoll*, 99 Mass. 281), are said to be exceptions to a general rule. On the other hand, injury to feelings is a recognized element of damages in actions of slander and libel, and of malicious prosecution. These distinctions between the cases, where injury to feelings does and where it does not constitute a cause of action or legal element of damages, are not logical, but doubtless serve well as practical rules. It will, it is believed, be found, upon examination of the authorities, that wherever substantial mental suffering would be the natural and probable result of the act, there compensation for injury to feelings has been allowed, and that where no mental suffering would ordinarily result, or if resulting, would naturally be but trifling, and being unaccompanied by visible signs of injury, would afford a wide scope for imaginative ills, there damages have been disallowed. The decisions on this subject illustrate well the subjection in our law of logic to common-sense.

¹ "Injuria, in the narrower sense, is every intentional and illegal violation of honour, i.e., the whole personality of another." "Now an outrage is committed not only when a man shall be struck with the fist, say, or with a club, or even flogged, but also if abusive language has been used to one." Salkowski, *Roman Law*, p. 668 and p. 669, n. 2.

² "It is certain every man has a right to keep his own sentiments, if he pleases. He has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends." Yates, J., in *Millar v. Taylor*, 4 Burr. 2303, 2379 (1769).

method of expression adopted. It is immaterial whether it be by word¹ or by signs,² in painting,³ by sculpture, or in music.⁴ Neither does the existence of the right depend upon the nature or value of the thought or emotion, nor upon the excellence of the means of expression.⁵ The same protection is accorded to a casual letter or an entry in a diary and to the most valuable poem or essay, to a botch or daub and to a masterpiece. In every such case the individual is entitled to decide whether that which is his shall be given to the public.⁶ No other has the right to publish his productions in any form, without his consent. This right is wholly independent of the material on which, or the means by which, the thought, sentiment, or emotion is expressed. It may exist independently of any corporeal being, as in words spoken, a song sung, a drama acted. Or if expressed on any material, as a poem in writing, the author may have parted with the paper, without forfeiting any proprietary right in the composition itself. The right is lost only when the author himself communicates his production to the public,—in other words,

¹ Nicols *v.* Pitman, 26 Ch. D. 374 (1884).

² Lee *v.* Simpson, 3 C. B. 871, 881; Daly *v.* Palmer, 6 Blatchf. 256.

³ Turner *v.* Robinson, 10 Ir. Ch. 121; s. c. ib. 510.

⁴ *Drone on Copyright*, 102.

⁵ “Assuming the law to be so, what is its foundation in this respect? It is not, I conceive, referable to any consideration peculiarly literary. Those with whom our common law originated had not probably among their many merits that of being patrons of letters; but they knew the duty and necessity of protecting property, and with that general object laid down rules providently expansive,—rules capable of adapting themselves to the various forms and modes of property which peace and cultivation might discover and introduce.

“The produce of mental labor, thoughts and sentiments, recorded and preserved by writing, became, as knowledge went onward and spread, and the culture of man’s understanding advanced, a kind of property impossible to disregard, and the interference of modern legislation upon the subject, by the stat. 8 Anne, professing by its title to be ‘For the encouragement of learning,’ and using the words ‘taken the liberty,’ in the preamble, whether it operated in augmentation or diminution of the private rights of authors, having left them to some extent untouched, it was found that the common law, in providing for the protection of property, provided for their security, at least before general publication by the writer’s consent.” Knight Bruce, V. C., in *Prince Albert v. Strange*, 2 DeGex & Sm. 652, 695 (1849).

⁶ “The question, however, does not turn upon the form or amount of mischief or advantage, loss or gain. The author of manuscripts, whether he is famous or obscure, low or high, has a right to say of them, if innocent, that whether interesting or dull, light or heavy, saleable or unsaleable, they shall not, without his consent, be published.” Knight Bruce, V. C., in *Prince Albert v. Strange*, 2 DeGex & Sm. 652, 694.

publishes it.¹ It is entirely independent of the copyright laws, and their extension into the domain of art. The aim of those statutes is to secure to the author, composer, or artist the entire profits arising from publication; but the common-law protection enables him to control absolutely the act of publication, and in the exercise of his own discretion, to decide whether there shall be any publication at all.² The statutory right is of no value, *unless* there is a publication; the common-law right is lost *as soon as* there is a publication.

What is the nature, the basis, of this right to prevent the publication of manuscripts or works of art? It is stated to be the enforcement of a right of property;³ and no difficulty arises in accepting this view, so long as we have only to deal with the reproduction of literary and artistic compositions. They certainly possess many of the attributes of ordinary property: they are transferable; they have a value; and publication or reproduction is a use by which that value is realized. But where the value of the production is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all, it is difficult to regard the right as one of property, in the common acceptation

¹ Duke of Queensberry *v.* Shebbeare, ² Eden, 329 (1758); Bartlett *v.* Crittenden, 5 McLean, 32, 41 (1849).

² *Drone on Copyright*, pp. 102, 104; Parton *v.* Prang, 3 Clifford, 537, 548 (1872); Jefferys *v.* Boosey, 4 H. L. C. 815, 867, 962 (1854).

³ "The question will be whether the bill has stated facts of which the court can take notice, as a case of civil property, which it is bound to protect. The injunction cannot be maintained on any principle of this sort, that if a letter has been written in the way of friendship, either the continuance or the discontinuance of the friendship affords a reason for the interference of the court." Lord Eldon in *Gee v. Pritchard*, 2 Swanst. 402, 413 (1818).

"Upon the principle, therefore, of protecting property, it is that the common law, in cases not aided or prejudiced by statute, shelters the privacy and seclusion of thought and sentiments committed to writing, and desired by the author to remain not generally known." Knight Bruce, V. C., in *Prince Albert v. Strange*, 2 DeGex & Sm. 652, 695.

"It being conceded that reasons of expediency and public policy can never be made the sole basis of civil jurisdiction, the question, whether upon any ground the plaintiff can be entitled to the relief which he claims, remains to be answered; and it appears to us that there is only one ground upon which his title to claim, and our jurisdiction to grant, the relief, can be placed. We must be satisfied, that the publication of private letters, without the consent of the writer, is an invasion of an exclusive right of property which remains in the writer, even when the letters have been sent to, and are still in the possession of his correspondent." Duer, J., in *Woolsey, v. Judd*, 4 Duer, 379, 384 (1855).

of that term. A man records in a letter to his son, or in his diary, that he did not dine with his wife on a certain day. No one into whose hands those papers fall could publish them to the world, even if possession of the documents had been obtained rightfully ; and the prohibition would not be confined to the publication of a copy of the letter itself, or of the diary entry ; the restraint extends also to a publication of the contents. What is the thing which is protected ? Surely, not the intellectual act of recording the fact that the husband did not dine with his wife, but that fact itself. It is not the intellectual product, but the domestic occurrence. A man writes a dozen letters to different people. No person would be permitted to publish a list of the letters written. If the letters or the contents of the diary were protected as literary compositions, the scope of the protection afforded should be the same secured to a published writing under the copyright law. But the copyright law would not prevent an enumeration of the letters, or the publication of some of the facts contained therein. The copyright of a series of paintings or etchings would prevent a reproduction of the paintings as pictures ; but it would not prevent a publication of a list or even a description of them.¹ Yet in the famous case of

¹ "A work lawfully published, in the popular sense of the term, stands in this respect, I conceive, differently from a work which has never been in that situation. The former may be liable to be translated, abridged, analyzed, exhibited in morsels, complimented, and otherwise treated, in a manner that the latter is not.

"Suppose, however,— instead of a translation, an abridgment, or a review,— the case of a catalogue,— suppose a man to have composed a variety of literary works ('innocent,' to use Lord Eldon's expression), which he has never printed or published, or lost the right to prohibit from being published,— suppose a knowledge of them unduly obtained by some unscrupulous person, who prints with a view to circulation a descriptive catalogue, or even a mere list of the manuscripts, without authority or consent, does the law allow this? I hope and believe not. The same principles that prevent more candid piracy must, I conceive, govern such a case also.

"By publishing of a man that he has written to particular persons, or on particular subjects, he may be exposed, not merely to sarcasm, he may be ruined. There may be in his possession returned letters that he had written to former correspondents, with whom to have had relations, however harmlessly, may not in after life be a recommendation; or his writings may be otherwise of a kind squaring in no sort with his outward habits and worldly position. There are callings even now in which to be convicted of literature, is dangerous, though the danger is sometimes escaped.

"Again, the manuscripts may be those of a man on account of whose name alone a mere list would be matter of general curiosity. How many persons could be mentioned, a catalogue of whose unpublished writings would, during their lives or afterwards, command a ready sale!" Knight Bruce, V. C., in *Prince Albert v. Strange*, 2 De Gex & Sm. 652, 693.

Prince Albert *v.* Strange, the court held that the common-law rule prohibited not merely the reproduction of the etchings which the plaintiff and Queen Victoria had made for their own pleasure, but also "the publishing (at least by printing or writing), though not by copy or resemblance, a description of them, whether more or less limited or summary, whether in the form of a catalogue or otherwise."¹ Likewise, an unpublished collection of news possessing no element of a literary nature is protected from piracy.²

That this protection cannot rest upon the right to literary or artistic property in any exact sense, appears the more clearly

¹ "A copy or impression of the etchings would only be a means of communicating knowledge and information of the original, and does not a list and description of the same? The means are different, but the object and effect are similar; for in both, the object and effect is to make known to the public more or less of the unpublished work and composition of the author, which he is entitled to keep wholly for his private use and pleasure, and to withhold altogether, or so far as he may please, from the knowledge of others. Cases upon abridgments, translations, extracts, and criticisms of published works have no reference whatever to the present question; they all depend upon the extent of right under the acts respecting copyright, and have no analogy to the exclusive rights in the author of unpublished compositions which depend entirely upon the common-law right of property." Lord Cottenham in Prince Albert *v.* Strange, 1 McN. & G. 23, 43 (1849). "Mr. Justice Yates, in Millar *v.* Taylor, said, that an author's case was exactly similar to that of an inventor of a new mechanical machine; that both original inventions stood upon the same footing in point of property, whether the case were mechanical or literary, whether an epic poem or an orrery; that the immorality of pirating another man's invention was as great as that of purloining his ideas. Property in mechanical works or works of art, executed by a man for his own amusement, instruction, or use, is allowed to subsist, certainly, and may, before publication by him, be invaded, not merely by copying, but by description or by catalogue, as it appears to me. A catalogue of such works may in itself be valuable. It may also as effectually show the bent and turn of the mind, the feelings and taste of the artist, especially if not professional, as a list of his papers. The portfolio or the studio may declare as much as the writing-table. A man may employ himself in private in a manner very harmless, but which, disclosed to society, may destroy the comfort of his life, or even his success in it. Every one, however, has a right, I apprehend, to say that the produce of his private hours is not more liable to publication without his consent, because the publication must be creditable or advantageous to him, than it would be in opposite circumstances."

"I think, therefore, not only that the defendant here is unlawfully invading the plaintiff's rights, but also that the invasion is of such a kind and affects such property as to entitle the plaintiff to the preventive remedy of an injunction; and if not the more, yet, certainly, not the less, because it is an intrusion,—an unbecoming and unseemly intrusion,—an intrusion not alone in breach of conventional rules, but offensive to that inbred sense of propriety natural to every man,—if intrusion, indeed, fitly describes a sordid spying into the privacy of domestic life,—into the home (a word hitherto sacred among us), the home of a family whose life and conduct form an acknowledged title, though not their only unquestionable title, to the most marked respect in this country." Knight Bruce, V. C., in Prince Albert *v.* Strange, 2 DeGex & Sm. 652, 696, 697.

² Kiernan *v.* Manhattan Quotation Co., 50 How. Pr. 194 (1876).

when the subject-matter for which protection is invoked is not even in the form of intellectual property, but has the attributes of ordinary tangible property. Suppose a man has a collection of gems or curiosities which he keeps private: it would hardly be contended that any person could publish a catalogue of them, and yet the articles enumerated are certainly not intellectual property in the legal sense, any more than a collection of stoves or of chairs.¹

The belief that the idea of property in its narrow sense was the basis of the protection of unpublished manuscripts led an able court to refuse, in several cases, injunctions against the publication of private letters, on the ground that "letters not possessing the attributes of literary compositions are not property entitled to protection;" and that it was "evident the plaintiff could not have considered the letters as of any value whatever as literary productions, for a letter cannot be considered of value to the author which he never would consent to have published."² But

¹ "The defendants' counsel say, that a man acquiring a knowledge of another's property without his consent is not by any rule or principle which a court of justice can apply (however secretly he may have kept or endeavored to keep it) forbidden without his consent to communicate and publish that knowledge to the world, to inform the world what the property is, or to describe it publicly, whether orally, or in print or writing.

"I claim, however, leave to doubt whether, as to property of a private nature, which the owner, without infringing on the right of any other, may and does retain in a state of privacy, it is certain that a person who, without the owner's consent, express or implied, acquires a knowledge of it, can lawfully avail himself of the knowledge so acquired to publish without his consent a description of the property.

"It is probably true that such a publication may be in a manner or relate to property of a kind rendering a question concerning the lawfulness of the act too slight to deserve attention. I can conceive cases, however, in which an act of the sort may be so circumstanced or relate to property such, that the matter may weightily affect the owner's interest or feelings, or both. For instance, the nature and intention of an unfinished work of an artist, prematurely made known to the world, may be painful and deeply prejudicial against him; nor would it be difficult to suggest other examples. . . .

"It was suggested that, to publish a catalogue of a collector's gems, coins, antiquities, or other such curiosities, for instance, without his consent, would be to make use of his property without his consent; and it is true, certainly, that a proceeding of that kind may not only as much embitter one collector's life as it would flatter another,—may be not only an ideal calamity,—but may do the owner damage in the most vulgar sense. Such catalogues, even when not descriptive, are often sought after, and sometimes obtain very substantial prices. These, therefore, and the like instances, are not necessarily examples merely of pain inflicted in point of sentiment or imagination; they may be that, and something else beside." Knight Bruce, V. C., in *Prince Albert v. Strange*, 2 DeGex & Sm. 652, 689, 690.

² *Hoyt v. Mackenzie*, 3 Barb. Ch. 320, 324 (1848); *Wetmore v. Scovell*, 3 Edw. Ch. 515 (1842). See Sir Thomas Plumer in 2 Ves. & B. 19 (1813).

these decisions have not been followed,¹ and it may now be considered settled that the protection afforded by the common law to the author of any writing is entirely independent of its pecuniary value, its intrinsic merits, or of any intention to publish the same, and, of course, also, wholly independent of the material, if any, upon which, or the mode in which, the thought or sentiment was expressed.

Although the courts have asserted that they rested their decisions on the narrow grounds of protection to property, yet there are recognitions of a more liberal doctrine. Thus in the case of *Prince Albert v. Strange*, already referred to, the opinions both of the Vice-Chancellor and of the Lord Chancellor, on appeal, show a more or less clearly defined perception of a principle broader than those which were mainly discussed, and on which they both placed their chief reliance. Vice-Chancellor Knight Bruce referred to publishing of a man that he had "written to particular persons or on particular subjects" as an instance of possibly injurious disclosures as to private matters, that the courts would in a proper case prevent; yet it is difficult to perceive how, in such a case, any right of property, in the narrow sense, would be drawn in question, or why, if such a publication would be restrained when it threatened to expose the victim not merely to sarcasm, but to ruin, it should not equally be enjoined, if it threatened to embitter his life. To deprive a man of the potential profits to be realized by publishing a catalogue of his gems cannot *per se* be a wrong to him. The possibility of future profits is not a right of property which the law ordinarily recognizes; it must, therefore, be an infraction of other rights which constitutes the wrongful act, and that infraction is equally wrongful, whether its results are to forestall the profits that the individual himself might secure by giving the matter a publicity obnoxious to him, or to gain an advantage at the expense of his mental pain and suffering. If the fiction of property in a narrow sense must be preserved, it is still true that the end accomplished by the gossip-monger is attained by the use of that which

¹ *Woolsey v. Judd*, 4 Duer, 379, 404 (1855). "It has been decided, fortunately for the welfare of society, that the writer of letters, though written without any purpose of profit, or any idea of literary property, possesses such a right of property in them, that they cannot be published without his consent, unless the purposes of justice, civil or criminal, require the publication." Sir Samuel Romilly, *arg.*, in *Gee v. Pritchard*, 2 Swanst. 402, 418 (1818). But see *High on Injunctions*, 3d ed., § 1012, *contra*.

is another's, the facts relating to his private life, which he has seen fit to keep private. Lord Cottenham stated that a man "is entitled to be protected in the exclusive use and enjoyment of that which is exclusively his," and cited with approval the opinion of Lord Eldon, as reported in a manuscript note of the case of *Wyatt v. Wilson*, in 1820, respecting an engraving of George the Third during his illness, to the effect that "if one of the late king's physicians had kept a diary of what he heard and saw, the court would not, in the king's lifetime, have permitted him to print and publish it;" and Lord Cottenham declared, in respect to the acts of the defendants in the case before him, that "privacy is the right invaded." But if privacy is once recognized as a right entitled to legal protection, the interposition of the courts cannot depend on the particular nature of the injuries resulting.

These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed—and (as that is the distinguishing attribute of property) there may be some propriety in speaking of those rights as property. But, obviously, they bear little resemblance to what is ordinarily comprehended under that term. The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.¹

¹ "But a doubt has been suggested, whether mere private letters, not intended as literary compositions, are entitled to the protection of an injunction in the same manner as compositions of a literary character. This doubt has probably arisen from the habit of not discriminating between the different rights of property which belong to an unpublished manuscript, and those which belong to a published book. The latter, as I have intimated in another connection, is a right to take the profits of publication. The former is a right to control the act of publication, and to decide whether there shall be any publication at all. It has been called a right of property; an expression perhaps not quite satisfactory, but on the other hand sufficiently descriptive of a right which, however incorporeal, involves many of the essential elements of property, and is at least positive and definite. This expression can leave us in no doubt as to the meaning of the learned

If we are correct in this conclusion, the existing law affords a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds. For the protection afforded is not confined by the authorities to those cases where any particular medium or form of expression has been adopted, nor to products of the intellect. The same protection is afforded to emotions and sensations expressed in a musical composition or other work of art as to a literary composition; and words spoken, a pantomime acted, a sonata performed, is no less entitled to protection than if each had been reduced to writing. The circumstance that a thought or emotion has been recorded in a permanent form renders its identification easier, and hence may be important from the point of view of evidence, but it has no significance as a matter of substantive right. If, then, the decisions indicate a general right to privacy for thoughts, emotions, and sensations, these should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression.

It may be urged that a distinction should be taken between the

judges who have used it, when they have applied it to cases of unpublished manuscripts. They obviously intended to use it in no other sense, than in contradistinction to the mere interests of feeling, and to describe a substantial right of legal interest." Curtis on Copyright, pp. 93, 94.

The resemblance of the right to prevent publication of an unpublished manuscript to the well-recognized rights of personal immunity is found in the treatment of it in connection with the rights of creditors. The right to prevent such publication and the right of action for its infringement, like the cause of action for an assault, battery, defamation, or malicious prosecution, are not assets available to creditors.

"There is no law which can compel an author to publish. No one can determine this essential matter of publication but the author. His manuscripts, however valuable, cannot, without his consent, be seized by his creditors as property." McLean, J., in Bartlett *v.* Crittenden, 5 McLean, 32, 37 (1849).

It has also been held that even where the sender's rights are not asserted, the receiver of a letter has not such property in it as passes to his executor or administrator as a salable asset. *Eyre v. Higbee*, 22 How. Pr. (N. Y.) 198 (1861).

"The very meaning of the word 'property' in its legal sense is 'that which is peculiar or proper to any person; that which belongs exclusively to one.' The first meaning of the word from which it is derived — *proprius* — is 'one's own.'" Drone on Copyright, p. 6.

It is clear that a thing must be capable of identification in order to be the subject of exclusive ownership. But when its identity can be determined so that individual ownership may be asserted, it matters not whether it be corporeal or incorporeal.

deliberate expression of thoughts and emotions in literary or artistic compositions and the casual and often involuntary expression given to them in the ordinary conduct of life. In other words, it may be contended that the protection afforded is granted to the conscious products of labor, perhaps as an encouragement to effort.¹ This contention, however plausible, has, in fact, little to recommend it. If the amount of labor involved be adopted as the test, we might well find that the effort to conduct one's self properly in business and in domestic relations had been far greater than that involved in painting a picture or writing a book; one would find that it was far easier to express lofty sentiments in a diary than in the conduct of a noble life. If the test of deliberateness of the act be adopted, much casual correspondence which is now accorded full protection would be excluded from the beneficent operation of existing rules. After the decisions denying the distinction attempted to be made between those literary productions which it was intended to publish and those which it was not, all considerations of the amount of labor involved, the degree of deliberation, the value of the product, and the intention of publishing must be abandoned, and no basis is discerned upon which the right to restrain publication and reproduction of such so-called literary and artistic works can be rested, except the right to privacy, as a part of the more general right to the immunity of the person, — the right to one's personality.

It should be stated that, in some instances where protection has been afforded against wrongful publication, the jurisdiction has been asserted, not on the ground of property, or at least not wholly on that ground, but upon the ground of an alleged breach of an implied contract or of a trust or confidence.

Thus, in *Abernethy v. Hutchinson*, 3 L. J. Ch. 209 (1825), where the plaintiff, a distinguished surgeon, sought to restrain the publication in the "Lancet" of unpublished lectures which he had delivered at St. Batholomew's Hospital in London, Lord Eldon

¹ "Such then being, as I believe, the nature and the foundation of the common law as to manuscripts independently of Parliamentary additions and subtractions, its operation cannot of necessity be confined to literary subjects. That would be to limit the rule by the example. Wherever the produce of labor is liable to invasion in an analogous manner, there must, I suppose, be a title to analogous protection or redress." *Knight Bruce, V. C., in Prince Albert v. Strange*, 2 DeGex & Sm. 652, 696.

doubted whether there could be property in lectures which had not been reduced to writing, but granted the injunction on the ground of breach of confidence, holding "that when persons were admitted as pupils or otherwise, to hear these lectures, although they were orally delivered, and although the parties might go to the extent, if they were able to do so, of putting down the whole by means of short-hand, yet they could do that only for the purposes of their own information, and could not publish, for profit, that which they had not obtained the right of selling."

In *Prince Albert v. Strange*, 1 *McN. & G.* 25 (1849), Lord Cottenham, on appeal, while recognizing a right of property in the etchings which of itself would justify the issuance of the injunction, stated, after discussing the evidence, that he was bound to assume that the possession of the etchings by the defendant had "its foundation in a breach of trust, confidence, or contract," and that upon such ground also the plaintiff's title to the injunction was fully sustained.

In *Tuck v. Priester*, 19 *Q. B. D.* 639 (1887), the plaintiffs were owners of a picture, and employed the defendant to make a certain number of copies. He did so, and made also a number of other copies for himself, and offered them for sale in England at a lower price. Subsequently, the plaintiffs registered their copyright in the picture, and then brought suit for an injunction and damages. The Lords Justices differed as to the application of the copyright acts to the case, but held unanimously that independently of those acts, the plaintiffs were entitled to an injunction and damages for breach of contract.

In *Pollard v. Photographic Co.*, 40 *Ch. Div.* 345 (1888), a photographer who had taken a lady's photograph under the ordinary circumstances was restrained from exhibiting it, and also from selling copies of it, on the ground that it was a breach of an implied term in the contract, and also that it was a breach of confidence. Mr. Justice North interjected in the argument of the plaintiff's counsel the inquiry: "Do you dispute that if the negative likeness were taken on the sly, the person who took it might exhibit copies?" and counsel for the plaintiff answered: "In that case there would be no trust or consideration to support a contract." Later, the defendant's counsel argued that "a person has no property in his own features; short of doing what is libellous or otherwise illegal, there is no restriction on the

photographer's using his negative." But the court, while expressly finding a breach of contract and of trust sufficient to justify its interposition, still seems to have felt the necessity of resting the decision also upon a right of property,¹ in order to

¹ "The question, therefore, is whether a photographer who has been employed by a customer to take his or her portrait is justified in striking off copies of such photograph for his own use, and selling and disposing of them, or publicly exhibiting them by way of advertisement or otherwise, without the authority of such customer, either express or implied. I say 'express or implied,' because a photographer is frequently allowed, on his own request, to take a photograph of a person under circumstances in which a subsequent sale by him must have been in the contemplation of both parties, though not actually mentioned. To the question thus put, my answer is in the negative, that the photographer is not justified in so doing. Where a person obtains information in the course of a confidential employment, the law does not permit him to make any improper use of the information so obtained; and an injunction is granted, if necessary, to restrain such use; as, for instance, to restrain a clerk from disclosing his master's accounts, or an attorney from making known his client's affairs, learned in the course of such employment. Again, the law is clear that a breach of contract, whether express or implied, can be restrained by injunction. In my opinion the case of the photographer comes within the principles upon which both these classes of cases depend. The object for which he is employed and paid is to supply his customer with the required number of printed photographs of a given subject. For this purpose the negative is taken by the photographer on glass; and from this negative copies can be printed in much larger numbers than are generally required by the customer. The customer who sits for the negative thus puts the power of reproducing the object in the hands of the photographer; and in my opinion the photographer who uses the negative to produce other copies for his own use, without authority, is abusing the power confidentially placed in his hands merely for the purpose of supplying the customer; and further, I hold that the bargain between the customer and the photographer includes, by implication, an agreement that the prints taken from the negative are to be appropriated to the use of the customer only." Referring to the opinions delivered in *Tuck v. Priester*, 19 Q. B. D. 639, the learned justice continued: "Then Lord Justice Lindley says: 'I will deal first with the injunction, which stands, or may stand, on a totally different footing from either the penalties or the damages. It appears to me that the relation between the plaintiffs and the defendant was such that, whether the plaintiffs had any copyright or not, the defendant has done that which renders him liable to an injunction. He was employed by the plaintiffs to make a certain number of copies of the picture, and that employment carried with it the necessary implication that the defendant was not to make more copies for himself, or to sell the additional copies in this country in competition with his employer. Such conduct on his part is a gross breach of contract and a gross breach of faith, and, in my judgment, clearly entitles the plaintiffs to an injunction, whether they have a copyright in the picture or not.' That case is the more noticeable, as the contract was in writing; and yet it was held to be an implied condition that the defendant should not make any copies for himself. The phrase 'a gross breach of faith' used by Lord Justice Lindley in that case applies with equal force to the present, when a lady's feelings are shocked by finding that the photographer she has employed to take her likeness for her own use is publicly exhibiting and selling copies thereof." North, J., in *Pollard v. L'photographic Co.*, 40 Ch. D. 345, 349-352 (1888).

"It may be said also that the cases to which I have referred are all cases in which there was some right of property infringed, based upon the recognition by the law of pro-

bring it within the line of those cases which were relied upon as precedents.¹

This process of implying a term in a contract, or of implying a trust (particularly where the contract is written, and where there is no established usage or custom), is nothing more nor less than a judicial declaration that public morality, private justice, and general convenience demand the recognition of such a rule, and that the publication under similar circumstances would be considered an intolerable abuse. So long as these circumstances happen to present a contract upon which such a term can be engrafted by the judicial mind, or to supply relations upon which a trust or confidence can be erected, there may be no objection to working out the desired protection through the doctrines of contract or of trust. But the court can hardly stop there. The narrower doctrine may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special

tection being due for the products of a man's own skill or mental labor; whereas in the present case the person photographed has done nothing to merit such protection, which is meant to prevent legal wrongs, and not mere sentimental grievances. But a person whose photograph is taken by a photographer is not thus deserted by the law; for the Act of 25 and 26 Vict., c. 68, s. 1, provides that when the negative of any photograph is made or executed for or on behalf of another person for a good or valuable consideration, the person making or executing the same shall not retain the copyright thereof, unless it is expressly reserved to him by agreement in writing signed by the person for or on whose behalf the same is so made or executed; but the copyright shall belong to the person for or on whose behalf the same shall have been made or executed.

"The result is that in the present case the copyright in the photograph is in one of the plaintiffs. It is true, no doubt, that sect. 4 of the same act provides that no proprietor of copyright shall be entitled to the benefit of the act until registration, and no action shall be sustained in respect of anything done before registration; and it was, I presume, because the photograph of the female plaintiff has not been registered that this act was not referred to by counsel in the course of the argument. But, although the protection against the world in general conferred by the act cannot be enforced until after registration, this does not deprive the plaintiffs of their common-law right of action against the defendant for his breach of contract and breach of faith. This is quite clear from the cases of *Morison v. Moat* [9 Hare, 241] and *Tuck v. Priester* [19 Q. B. D. 629] already referred to, in which latter case the same act of Parliament was in question." Per North, J., *ibid.* p. 352.

This language suggests that the property right in photographs or portraits may be one created by statute, which would not exist in the absence of registration; but it is submitted that it must eventually be held here, as it has been in the similar cases, that the statute provision becomes applicable only when there is a publication, and that before the act of registering there is property in the thing upon which the statute is to operate.

¹ *Duke of Queensberry v. Shebbeare*, 2 *Eden*, 329; *Murray v. Heath*, 1 *B. & Ad.* 804; *Tuck v. Priester*, 19 *Q. B. D.* 629.

confidence; but now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation. While, for instance, the state of the photographic art was such that one's picture could seldom be taken without his consciously "sitting" for the purpose, the law of contract or of trust might afford the prudent man sufficient safeguards against the improper circulation of his portrait; but since the latest advances in photographic art have rendered it possible to take pictures surreptitiously, the doctrines of contract and of trust are inadequate to support the required protection, and the law of tort must be resorted to. The right of property in its widest sense, including all possession, including all rights and privileges, and hence embracing the right to an inviolate personality, affords alone that broad basis upon which the protection which the individual demands can be rested.

Thus, the courts, in searching for some principle upon which the publication of private letters could be enjoined, naturally came upon the ideas of a breach of confidence, and of an implied contract; but it required little consideration to discern that this doctrine could not afford all the protection required, since it would not support the court in granting a remedy against a stranger; and so the theory of property in the contents of letters was adopted.¹ Indeed, it is difficult to conceive on what theory of the law the casual recipient of a letter, who proceeds to publish it, is guilty of a breach of contract, express or implied, or of any breach of trust, in the ordinary acceptation of that term. Suppose a letter has been addressed to him without his solicitation. He opens it, and reads. Surely, he has not made any contract; he has not accepted any trust. He cannot, by opening and reading

¹See Mr. Justice Story in *Folsom v. Marsh*, 2 Story, 100, 111 (1841):—

"If he [the recipient of a letter] attempt to publish such letter or letters on other occasions, not justifiable, a court of equity will prevent the publication by an injunction, as a breach of private confidence or contract, or of the rights of the author; and *a fortiori*, if he attempt to publish them for profit; for then it is not a mere breach of confidence or contract, but it is a violation of the exclusive copyright of the writer. . . . The general property, and the general rights incident to property, belong to the writer, whether the letters are literary compositions, or familiar letters, or details of facts, or letters of business. The general property in the manuscripts remains in the writer and his representatives, as well as the general copyright. *A fortiori*, third persons, standing in no privity with either party, are not entitled to publish them, to subserve their own private purposes of interest, or curiosity, or passion."

the letter, have come under any obligation save what the law declares; and, however expressed, that obligation is simply to observe the legal right of the sender, whatever it may be, and whether it be called his right of property in the contents of the letter, or his right to privacy.¹

A similar groping for the principle upon which a wrongful publication can be enjoined is found in the law of trade secrets. There, injunctions have generally been granted on the theory of a breach of contract, or of an abuse of confidence.² It would, of course, rarely happen that any one would be in the possession of a secret unless confidence had been reposed in him. But can it be supposed that the court would hesitate to grant relief against one who had obtained his knowledge by an ordinary trespass,—for instance, by wrongfully looking into a book in which the secret was recorded, or by eavesdropping? Indeed, in *Yovatt v. Winyard*, 1 J. & W. 394 (1820), where an injunction was granted against making any use of or communicating certain recipes for veterinary medicine, it appeared that the defendant, while in the plaintiff's employ, had surreptitiously got access to his book of recipes, and copied them. Lord Eldon "granted the injunction, upon the ground of there having been a breach of trust and confidence;" but it would seem to be difficult to draw any sound legal distinction between such a case and one where a mere stranger wrongfully obtained access to the book.³

¹ "The receiver of a letter is not a bailee, nor does he stand in a character analogous to that of a bailee. There is no right to possession, present or future, in the writer. The only right to be enforced against the holder is a right to prevent publication, not to require the manuscript from the holder in order to a publication of himself." Per Hon. Joel Parker, quoted in *Grigsby v. Breckenridge*, 2 Bush. 480, 489 (1857).

² In *Morison v. Moat*, 9 Hare, 241, 255 (1851), a suit for an injunction to restrain the use of a secret medical compound, Sir George James Turner, V. C., said: "That the court has exercised jurisdiction in cases of this nature does not, I think, admit of any question. Different grounds have indeed been assigned for the exercise of that jurisdiction. In some cases it has been referred to property, in others to contract, and in others, again, it has been treated as founded upon trust or confidence,—meaning, as I conceive, that the court fastens the obligation on the conscience of the party, and enforces it against him in the same manner as it enforces against a party to whom a benefit is given, the obligation of performing a promise on the faith of which the benefit has been conferred; but upon whatever grounds the jurisdiction is founded, the authorities leave no doubt as to the exercise of it."

³ A similar growth of the law showing the development of contractual rights into rights of property is found in the law of goodwill. There are indications, as early as the Year Books, of traders endeavoring to secure to themselves by contract the advantages now designated by the term "goodwill," but it was not until 1743 that goodwill received

We must therefore conclude that the rights, so protected, whatever their exact nature, are not rights arising from contract or from special trust, but are rights as against the world; and, as above stated, the principle which has been applied to protect these rights is in reality not the principle of private property, unless that word be used in an extended and unusual sense. The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise.¹

If the invasion of privacy constitutes a legal *injuria*, the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation.

The right of one who has remained a private individual, to prevent his public portraiture, presents the simplest case for such extension; the right to protect one's self from pen portraiture, from a discussion by the press of one's private affairs, would be a more important and far-reaching one. If casual and unimportant state-

legal recognition as property apart from the personal covenants of the traders. See Allan on Goodwill, pp. 2, 3.

¹ The application of an existing principle to a new state of facts is not judicial legislation. To call it such is to assert that the existing body of law consists practically of the statutes and decided cases, and to deny that the principles (of which these cases are ordinarily said to be evidence) exist at all. It is not the application of an existing principle to new cases, but the introduction of a new principle, which is properly termed judicial legislation.

But even the fact that a certain decision would involve judicial legislation should not be taken as conclusive against the propriety of making it. This power has been constantly exercised by our judges, when applying to a new subject principles of private justice, moral fitness, and public convenience. Indeed, the elasticity of our law, its adaptability to new conditions, the capacity for growth, which has enabled it to meet the wants of an ever changing society and to apply immediate relief for every recognized wrong, have been its greatest boast.

"I cannot understand how any person who has considered the subject can suppose that society could possibly have gone on if judges had not legislated, or that there is any danger whatever in allowing them that power which they have in fact exercised, to make up for the negligence or the incapacity of the avowed legislator. That part of the law of every country which was made by judges has been far better made than that part which consists of statutes enacted by the legislature." ¹ Austin's Jurisprudence, p. 224.

The cases referred to above show that the common law has for a century and a half protected privacy in certain cases, and to grant the further protection now suggested would be merely another application of an existing rule.

ments in a letter, if handiwork, however inartistic and valueless, if possessions of all sorts are protected not only against reproduction, but against description and enumeration, how much more should the acts and sayings of a man in his social and domestic relations be guarded from ruthless publicity. If you may not reproduce a woman's face photographically without her consent, how much less should be tolerated the reproduction of her face, her form, and her actions, by graphic descriptions colored to suit a gross and depraved imagination.

The right to privacy, limited as such right must necessarily be, has already found expression in the law of France.¹

It remains to consider what are the limitations of this right to privacy, and what remedies may be granted for the enforcement of the right. To determine in advance of experience the exact line at which the dignity and convenience of the individual must yield to the demands of the public welfare or of private justice would be a difficult task; but the more general rules are furnished by the legal analogies already developed in the law of slander and libel, and in the law of literary and artistic property.

i. The right to privacy does not prohibit any publication of matter which is of public or general interest.

In determining the scope of this rule, aid would be afforded by the analogy, in the law of libel and slander, of cases which deal with the qualified privilege of comment and criticism on matters of public and general interest.² There are of course difficulties in applying such a rule; but they are inherent in the subject-matter, and are certainly no greater than those which exist in many other branches of the law,—for instance, in that large class of cases in which the reasonableness or unreasonableness of an act is made the test of liability. The design of the law must be to protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity and to protect all persons, whatsoever; their position or station, from having matters which they may

¹ Loi Relative à la Presse, 11 Mai 1868.

"11. Toute publication dans un écrit périodique relative à un fait de la vie privée constitue une contravention punie d'un amende de cinq cent francs."

"La poursuite ne pourra être exercée que sur la plainte de la partie intéressée."

Rivière, Codes Français et Lois Usuelles, App. Code Pen., p. 20.

² See *Campbell v. Spottiswoode*, 3 B. & S. 769, 776; *Henwood v. Harrison*, L. R. 7 C. P. 606; *Gott v. Pulsifer*, 122 Mass. 235.

properly prefer to keep private, made public against their will. It is the unwarranted invasion of individual privacy which is reprehended, and to be, so far as possible, prevented. The distinction, however, noted in the above statement is obvious and fundamental. There are persons who may reasonably claim as a right, protection from the notoriety entailed by being made the victims of journalistic enterprise. There are others who, in varying degrees, have renounced the right to live their lives screened from public observation. Matters which men of the first class may justly contend, concern themselves alone, may in those of the second be the subject of legitimate interest to their fellow-citizens. Peculiarities of manner and person, which in the ordinary individual should be free from comment, may acquire a public importance, if found in a candidate for political office. Some further discrimination is necessary, therefore, than to class facts or deeds as public or private according to a standard to be applied to the fact or deed *per se*. To publish of a modest and retiring individual that he suffers from an impediment in his speech or that he cannot spell correctly, is an unwarranted, if not an unexampled, infringement of his rights, while to state and comment on the same characteristics found in a would-be congressman could not be regarded as beyond the pale of propriety.

The general object in view is to protect the privacy of private life, and to whatever degree and in whatever connection a man's life has ceased to be private, before the publication under consideration has been made, to that extent the protection is to be withdrawn.¹ Since, then, the propriety of publishing the very same facts may depend wholly upon the person concerning whom they are published, no fixed formula can be used to prohibit obnoxious publications. Any rule of liability adopted must have in it an elasticity which shall take account of the varying circumstances of each case,—a necessity which unfortunately renders such a doctrine not only more difficult of application, but also to

¹ " Nos moeurs n'admettent pas la prétention d'enlever aux investigations de la publicité les actes qui relèvent de la vie publique, et ce dernier mot ne doit pas être restreint à la vie officielle ou à celle du fonctionnaire. Tout homme qui appelle sur lui l'attention ou les regards du public, soit par une mission qu'il a reçue ou qu'il se donne, soit par le rôle qu'il s'attribue dans l'industrie, les arts, le théâtre, etc., ne peut plus invoquer contre la critique ou l'exposé de sa conduite d'autre protection que les lois qui répriment la diffamation et l'injure." Circ. Mins. Just., 4 Juin, 1868. Rivière Codes Français et Lois Usuelles, App. Code Pen. 20 n (b).

a certain extent uncertain in its operation and easily rendered abortive. Besides, it is only the more flagrant breaches of decency and propriety that could in practice be reached, and it is not perhaps desirable even to attempt to repress everything which the nicest taste and keenest sense of the respect due to private life would condemn.

In general, then, the matters of which the publication should be repressed may be described as those which concern the private life, habits, acts, and relations of an individual, and have no legitimate connection with his fitness for a public office which he seeks or for which he is suggested, or for any public or quasi public position which he seeks or for which he is suggested, and have no legitimate relation to or bearing upon any act done by him in a public or quasi public capacity. The foregoing is not designed as a wholly accurate or exhaustive definition, since that which must ultimately in a vast number of cases become a question of individual judgment and opinion is incapable of such definition; but it is an attempt to indicate broadly the class of matters referred to. Some things all men alike are entitled to keep from popular curiosity, whether in public life or not, while others are only private because the persons concerned have not assumed a position which makes their doings legitimate matters of public investigation.¹

2. The right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel.

Under this rule, the right to privacy is not invaded by any publication made in a court of justice, in legislative bodies, or the committees of those bodies; in municipal assemblies, or the committees of such assemblies, or practically by any communication made in any other public body, municipal or parochial, or in any body quasi public, like the large voluntary associations formed

¹ "Celui-la seul a droit au silence absolu qui n'a pas expressément ou indirectement provoqué ou autorisé l'attention, l'approbation ou le blâme." Circ. Mins. Just., 4 Juin, 1868. Rivière Codes Français et Lois Usuelles, App. Code Pen. 20 n (b).

The principle thus expressed evidently is designed to exclude the wholesale investigations into the past of prominent public men with which the American public is too familiar, and also, unhappily, too well pleased; while not entitled to the "silence *absolu*" which less prominent men may claim as their due, they may still demand that all the details of private life in its most limited sense shall not be laid bare for inspection.

for almost every purpose of benevolence, business, or other general interest ; and (at least in many jurisdictions) reports of any such proceedings would in some measure be accorded a like privilege.¹ Nor would the rule prohibit any publication made by one in the discharge of some public or private duty, whether legal or moral, or in conduct of one's own affairs, in matters where his own interest is concerned.²

3. The law would probably not grant any redress for the invasion of privacy by oral publication in the absence of special damage.

The same reasons exist for distinguishing between oral and written publications of private matters, as is afforded in the law of defamation by the restricted liability for slander as compared with the liability for libel.³ The injury resulting from such oral communications would ordinarily be so trifling that the law might well, in the interest of free speech, disregard it altogether.⁴

¹ Wason *v.* Walters, L. R. 4 Q. B. 73; Smith *v.* Higgins, 16 Gray, 251; Barrows *v.* Bell, 7 Gray, 331.

² This limitation upon the right to prevent the publication of private letters was recognized early : —

" But, consistently with this right [of the writer of letters], the persons to whom they are addressed may have, nay, must, by implication, possess, the right to publish any letter or letters addressed to them, upon such occasions, as require, or justify, the publication or public use of them ; but this right is strictly limited to such occasions. Thus, a person may justifiably use and publish, in a suit at law or in equity, such letter or letters as are necessary and proper, to establish his right to maintain the suit, or defend the same. So, if he be aspersed or misrepresented by the writer, or accused of improper conduct, in a public manner, he may publish such parts of such letter or letters, but no more, as may be necessary to vindicate his character and reputation, or free him from unjust obloquy and reproach." Story, J., in Folsom *v.* Marsh, 2 Story, 100, 110, 111 (1841).

The existence of any right in the recipient of letters to publish the same has been strenuously denied by Mr. Drone; but the reasoning upon which his denial rests does not seem satisfactory. Drone on Copyright, pp. 136-139.

³ Townshend on Slander and Libel, 4th ed., § 18; Odgers on Libel and Slander, 2d ed., p. 3.

⁴ " But as long as gossip was oral, it spread, as regards any one individual, over a very small area, and was confined to the immediate circle of his acquaintances. It did not reach, or but rarely reached, those who knew nothing of him. It did not make his name, or his walk, or his conversation familiar to strangers. And what is more to the purpose, it spared him the pain and mortification of knowing that he was gossipped about. A man seldom heard of oral gossip about him which simply made him ridiculous, or trespassed on his lawful privacy, but made no positive attack upon his reputation. His peace and comfort were, therefore, but slightly affected by it." E. L. Godkin, "The Rights of the Citizen : To his Reputation." Scribner's Magazine, July, 1890, p. 66.

Vice-Chancellor Knight Bruce suggested in Prince Albert *v.* Strange, 2 DeGex & Sm. 652, 694, that a distinction would be made as to the right to privacy of works of art between an oral and a written description or catalogue.

4. The right to privacy ceases upon the publication of the facts by the individual, or with his consent.

This is but another application of the rule which has become familiar in the law of literary and artistic property. The cases there decided establish also what should be deemed a publication, — the important principle in this connection being that a private communication of circulation for a restricted purpose is not a publication within the meaning of the law.¹

5. The truth of the matter published does not afford a defence. Obviously this branch of the law should have no concern with the truth of falsehood of the matters published. It is not for injury to the individual's character that redress or prevention is sought, but for injury to the right of privacy. For the former, the law of slander and libel provides perhaps a sufficient safeguard. The latter implies the right not merely to prevent inaccurate portrayal of private life, but to prevent its being depicted at all.²

6. The absence of "malice" in the publisher does not afford a defence.

Personal ill-will is not an ingredient of the offence, any more than in an ordinary case of trespass to person or to property. Such malice is never necessary to be shown in an action for libel or slander at common law, except in rebuttal of some defence, *e. g.*, that the occasion rendered the communication privileged, or, under the statutes in this State and elsewhere, that the statement complained of was true. The invasion of the privacy that is to be protected is equally complete and equally injurious, whether the motives by which the speaker or writer was actuated are, taken by themselves, culpable or not; just as the damage to character, and to some extent the tendency to provoke a breach of the peace, is equally the result of defamation without regard to the motives leading to its publication. Viewed as a wrong to the individual, this rule is the same pervading the whole law of torts, by which one is held responsible for his intentional acts, even though they are committed with no sinister intent; and viewed as a wrong

¹ See *Drone on Copyright*, pp. 121, 289, 290.

² Compare the French law.

"En prohibant l'enfâissement de la vie privée, sans qu'il soit nécessaire d'établir l'intention criminelle, la loi a entendue interdire toute discussion de la part de la défense sur la vérité des faits. Le remède eut été pire que le mal, si un débat avait pu s'engager sur ce terrain." Circ. Mins. Just., 4 Juin, 1868. *Rivière Code Français et Lois Usuelles*, App. Code Penn. 20 n(a).

to society, it is the same principle adopted in a large category of statutory offences.

The remedies for an invasion of the right of privacy are also suggested by those administered in the law of defamation, and in the law of literary and artistic property, namely :—

1. An action of tort for damages in all cases.¹ Even in the absence of special damages, substantial compensation could be allowed for injury to feelings as in the action of slander and libel.

2. An injunction, in perhaps a very limited class of cases.²

It would doubtless be desirable that the privacy of the individual should receive the added protection of the criminal law, but for this, legislation would be required.³ Perhaps it would be deemed proper to bring the criminal liability for such publication within narrower limits ; but that the community has an interest in preventing such invasions of privacy, sufficiently strong to justify the introduction of such a remedy, cannot be doubted. Still, the protection of society must come mainly through a recognition of

¹ Comp. *Drone on Copyright*, p. 107.

² *Comp. High on Injunctions*, 3d ed., § 1015; *Townshend on Libel and Slander*, 4th ed., §§ 417a-417d.

³ The following draft of a bill has been prepared by William H. Dunbar, Esq., of the Boston bar, as a suggestion for possible legislation :—

" SECTION 1. Whoever publishes in any newspaper, journal, magazine or other periodical publication any statement concerning the private life or affairs of another, after being requested in writing by such other person not to publish such statement or any statement concerning him, shall be punished by imprisonment in the State prison not exceeding five years, or by imprisonment in the jail not exceeding two years, or by fine not exceeding one thousand dollars ; provided, that no statement concerning the conduct of any person in, or the qualifications of any person for, a public office or position which such person holds, has held, or is seeking to obtain, or for which such person is at the time of such publication a candidate, or for which he or she is then suggested as a candidate, and no statement of or concerning the acts of any person in his or her business, profession, or calling, and no statement concerning any person in relation to a position, profession, business, or calling, bringing such person prominently before the public, or in relation to the qualifications for such a position, business, profession, or calling of any person prominent or seeking prominence before the public, and no statement relating to any act done by any person in a public place, nor any other statement of matter which is of public and general interest, shall be deemed a statement concerning the private life or affairs of such person within the meaning of this act.

" SECT. 2. It shall not be a defence to any criminal prosecution brought under section 1 of this act that the statement complained of is true, or that such statement was published without a malicious intention ; but no person shall be liable to punishment for any statement published under such circumstances that if it were defamatory the publication thereof would be privileged."

the rights of the individual. Each man is responsible for his own acts and omissions only. If he condones what he reprobates, with a weapon at hand equal to his defence, he is responsible for the results. If he resists, public opinion will rally to his support. Has he then such a weapon? It is believed that the common law provides him with one, forged in the slow fire of the centuries, and to-day fitly tempered to his hand. The common law has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?

*Samuel D. Warren,
Louis D. Brandeis.*

BOSTON, December, 1890.

Philosophica Law

AUTHORITY
EQUALITY
ADJUDICATION
PRIVACY

edited by Richard Bronaugh

Copyright © 1978 by Richard Bronaugh

All rights reserved. No portion of this book may
be reproduced, by any process or technique, without
the express written consent of the publisher.



Contributions in Legal Studies, Number 2

GREENWOOD PRESS

WESTPORT, CONNECTICUT • LONDON, ENGLAND

13

Privacy: some arguments and assumptions

RICHARD A. WASSERSTROM

In this paper I examine some issues involving privacy—issues with which the legal system of the United States has had and continues to have a good deal of concern.. What I am interested in is the nature of privacy and the reasons why it might be thought important. The issues I consider have been of particular interest in recent years as changes in technology have made new ways to interfere with privacy possible. For this reason, too, I am primarily concerned with the ways in which government and other powerful institutions can and do interfere with privacy, for it is these institutions that tend to have the sophisticated instruments most at their disposal.

I consider first some distinctions that I think it important to make among different kinds of cases that involve privacy. I then consider in some detail one plausible set of arguments for the value of privacy. These arguments help to explain why the law protects privacy in some of the ways it does and to provide a possible justification for continuing to do so. Some of the arguments are not without their problems, however. And in the final section of the article I raise certain questions about them and indicate the key issues that require additional exploration before any satisfactory justification can be developed.

It is apparent that there are a number of different claims that can be made in the name of privacy. A number—and perhaps all—of them involve the question of the kind and degree of control that a person ought to be able to exercise in respect to knowledge or the disclosure of information about himself or herself. This is not all there is to privacy, but it is surely one central theme.

It is also true that information about oneself is not all of the same type. As a result control over some kinds may be much more important than control over others. For this reason, I want to start by trying to identify some of the different types of information about oneself over which persons might desire to retain control, and I will describe the situations in which this information comes into being. To do this, I will consider four rather ordinary situations and look at the ways they resemble one another and differ from one another.

I

The cases I have in mind are these.

1. It is midafternoon and I am sitting in a chair resting. As I close my eyes and look inward, I become aware of numerous ideas running through my mind, of various emotions and feelings, and of a variety of bodily sensations—an itch on my scalp, a slight pain in my side, and so on.
2. I am in a closed telephone booth, no one is standing near the booth, and I am talking in a normal voice into the telephone. I have called my travel agent to find out what time there are flights to Chicago so that I can make a reservation for a trip.
3. I am in the bedroom of my home with my wife. We are both undressed, lying on the bed, having sexual intercourse.
4. I am considering hiring a research assistant for the summer. If I wish to, I dial a special number on the telephone and a few days later receive in the mail a computer printout consisting of a profile of the prospective assistant—her age, marital status, arrest record, if any, grades at school, income, as well as a summary of how she has spent her time over the past few years.

The first kind of case is that of the things that are going on within a person's head or body—especially, though, a person's head: his or her mental state. One thing that is significant about my dreams, my conscious thoughts, hopes, fears, and desires is that the most direct: the best, and often the only evidence for you of what they are consists in my deliberately revealing them to you. To be sure, my nonverbal behavior may give an observer a clue as to what is going on in my mind. If, for example, I have a faraway look in my eyes you may infer that I am daydreaming about something and not paying

very much attention to you. In addition there is, no doubt, a more intimate and even conceptual connection between observable behavior and certain states of feeling. If I am blushing that may mean that I am embarrassed. If I am talking very fast that may lead you to infer correctly that I am excited or nervous. It is also sometimes the case that I will not know my own thoughts and feelings and that by saying what I think they are, a skilled observer listening to me and watching me as I talk can tell better than can I what is really going on inside my head. This may be one way to describe what can take place during psychotherapy.

But even taking all of these qualifications into account, it still remains the case that the only way to obtain very detailed and accurate information about what I am thinking, fearing, imagining, desiring, or hating and how I am experiencing it is for me to tell you or show you. If I do not, the ideas and feeling remain within me and in some sense, at least, known only to me. Because people cannot read other people's minds, these things about me are known only to me in a way in which other things are not unless I decide to disclose them to you.

What about things that are going on in my body? In some respects the situation is similar to that of my thoughts and in some respects different. There are things that are going on in my body that are like my thoughts, fears, and fantasies. If I have a slight twinge of pain in my left big toe, there is no way for anyone else to know that unless I choose to disclose it. Of course, if the toe is swollen and red and if I grimace whenever I put any weight on it, an observer could doubtless infer correctly that I was experiencing pain there. But in many other cases the only evidence would be my verbal report.

There are other things about my body concerning which this privileged position does not obtain. Even though they are my ribs, I cannot tell very well what they look like; even though it is my blood, I cannot tell with any precision how much alcohol is there. A person looking through a fluoroscope at my ribs or at an x-ray of them can tell far better than I can (just from having them as my ribs or from looking down at my chest) what they look like. A trained technician looking at a sample of my blood in combination with certain chemicals can determine far better than I can (just from it being *my* blood)

what the alcohol content is or whether I am anemic.

So there are some facts about my body that I know in a way others logically cannot know them, that can be known to others only if I disclose them by telling what they are. There are other facts about my body that cannot be known by others in the way I know them but that can be inferred from observation of my body and my behavior. And there are still other kinds of facts about my body that I do not know and that can be learned, if at all, only by someone or something outside of myself.

The second kind of case was illustrated by an imagined telephone conversation from a phone booth with my travel agent to make the reservations for a trip. Another case of the same type is this: I am in the dining room of my house, the curtains are drawn, and I am eating dinner with my wife. In both of these cases it is the setting that makes the behavior distinctive and relevant for our purposes. In the example of the reservations over the telephone, the substance of my conversation with my travel agent is within my control if it is the case that no one is in a position to overhear (at my end) what I am saying to him, that no one is listening in along the way, and that only one person, the travel agent, is in a position to hear what I am telling him. It is less within my control, of course, than is information about my mental state, not yet revealed to anyone, because the agent can choose to reveal what I have told him.

In the second-case—that of eating dinner in my dining room—knowledge of what I am eating and how I am eating is in the control of my wife and me if it is correct that no one else is in a position to observe us as we are eating. We might want to describe both of these cases as cases of things being done *in private* (although this is a very weak sense of private)—meaning that they were done in a setting in which there did not appear to be anyone other than the person to whom I was talking or with whom I was eating who was in a position to hear what was being said or to see what was being eaten at the time the behavior was taking place. Both of these are to be contrasted with the third example given earlier.

Instead of eating dinner with my wife in the dining room, we are having sexual intercourse in the bedroom. Or, instead of talking to my travel agent, imagine that I call my lawyer to discuss the terms of my will with her. Both of these things are being done in private in

the same sense in which the discussion with the travel agent and the dinner with my wife were private. But these have an additional quality not possessed by the earlier two examples. While I expect that what I tell my lawyer is not being overheard by anyone else while I am telling her, I also reasonably expect that she will keep in confidence what I tell her. The conversation is private in the additional respect that the understanding is that it will not be subsequently disclosed to anyone without my consent. It is a private kind of communication. That is not the case with my phone reservations for Chicago. Absent special or unusual circumstances (for example, telling the agent that I do not want anyone to know when I am going to Chicago), I have no particular interest in retaining control over disclosure of this fact.

Similarly, having intercourse with my wife is private in the additional respect that it is the sort of intimate thing that is not appropriately observed by others or discussed with them—again, absent special or unusual circumstances. In addition to being done in private, it, too, is a private kind of thing. It is in this respect unlike the dinner we had together. There is no expectation on my part that what I ate or how I ate it will not be discussed with others by my wife.

The most obvious and the important connection between the idea of doing something in private and doing a private kind of thing is that we typically do private things only in situations where we reasonably believe that we are doing them in private. That we believe we are doing something in private is often a condition that has to be satisfied before we are willing to disclose an intimate fact about ourselves or to perform an intimate act. I would probably make my airplane reservations even in a crowded travel agency where there were lots of people who could overhear what I was saying. The telephone was a convenient way to make the reservations. But the fact that I was making them in a setting that appeared to be private was not important to me. It did not affect what I disclosed to the agent. Thus, even if I had suspected that my agent's telephone was tapped so that someone unknown to us both overheard our conversation, I would probably have made the reservation. In the case of my conversation with my lawyer, however, it was the belief that the conversation was in a private setting that made me willing to reveal a pri-

vate kind of information. If someone taped my discussion with my lawyer, he injured me in a way that is distinguishable on this basis alone from the injury, if any, done to me by taping my conversation with the travel agent. That is to say, he got me to do or to reveal something that I would not have done or revealed if they had not hidden his presence from me.

It should be evident, too, that there are important similarities, as well as some differences, between the first and third cases—between my knowledge of my own mental state and my disclosure of intimate or otherwise confidential information to those to whom I choose to disclose it. These can be brought out by considering what it would be like to live in a society whose technology permitted an observer to gain access to the information in question.

II

Suppose existing-technology made it possible for an outsider in some way to look into or monitor another's mind. What, if anything, would be especially disturbing or objectionable about that?

To begin with, there is a real sense in which we have far less control over when we shall have certain thoughts and what their content will be than we have over, for example, to whom we shall reveal them and to what degree. Because our inner thoughts, feelings, and bodily sensations are so largely beyond our control, I think we would feel appreciably more insecure in our social environment than we do at present were it possible for another to "look in" without our consent to see what was going on in our heads.

This is so at least in part because many, although by no means all, of our uncommunicated thoughts and feelings are about very intimate matters. Our fantasies and our fears often concern just those matters that in our culture we would least choose to reveal to anyone else. At a minimum we might suffer great anxiety and feelings of shame were the decisions as to where, when, and to whom we disclose not to be wholly ours. Were access to our thoughts possible in this way, we would see ourselves as creatures who are far more vulnerable than we are now.

In addition, there is a more straightforward worry about accountability for our thoughts and feelings. As I mentioned, they are often

not within our control. For all of the reasons that we ought not hold people accountable for behavior not within their control, we would not want the possibility of accountability to extend to uncommunicated thoughts and feelings.

Finally, one rather plausible conception of what it is to be a person carries with it the idea of the existence of a core of thoughts and feelings that are the person's alone. If anyone else could know all that I am thinking or perceive all that I am feeling except in the form I choose to filter and reveal what I am and how I see myself—if anyone could be aware of all this at will—I would cease to have as complete a sense of myself as a distinct and separate person as I have now. A fundamental part of what it is to be an individual is to be an entity that is capable of being exclusively aware of its own thoughts and feelings.

Considerations such as these—and particularly the last one—help us to understand some of the puzzles concerning the privilege against self-incrimination. Because of the significance of exclusive control over our own thoughts and feelings, the privilege against self-incrimination can be seen to rest, ultimately, upon a concern that confessions never be coerced or required by the state. The point of the privilege is not primarily that the state must be induced not to torture individuals in order to extract information from them. Nor is the point even essentially that the topics of confession will necessarily (or even typically) be of the type that we are most unwilling to disclose because of the unfavorable nature of what this would reveal about us. Rather, the fundamental point is that required disclosure of one's thoughts by itself diminishes the concept of individual personhood within the society. For this reason, all immunity statutes that require persons to reveal what they think and believe—provided only that they will not be subsequently prosecuted for what they disclose—are beside the point and properly subject to criticism. For this reason, too, cases that permit the taking of a blood sample (to determine alcohol content) from an unconscious or unwilling person—despite the existence of the privilege—are also defensible. Since a person is not in a privileged position in respect to the alcohol content of his or her own blood, the claim to exclusivity in respect to knowledge of this fact is not particularly persuasive.

In a society in which intrusion into the domain of one's uncommunicated thoughts and feelings was not possible, but in which communications between persons about private things could be intercepted, some of the problems would remain the same. To begin with, because of our social attitudes toward the disclosure of intimate facts and behavior, most of us would be extremely pained were we to learn that these had become known to persons other than those to whom we chose to disclose them. The pain can come about in several different ways. If I do something private with somebody and I believe that we are doing it in private, I may very well be hurt or embarrassed if I learn subsequently that we were observed but did not know it. Thus if I learn after the fact that someone had used a special kind of telescope to observe my wife and me while we were having intercourse, the knowledge that we were observed will cause us distress both because our expectations of privacy were incorrect and because we do not like the idea that we were observed during this kind of intimate act. People have the right to have the world be what it appears to be precisely in those cases in which they regard privacy as essential to the diminution of their own vulnerability.

Reasoning such as this lies behind, I think, a case that arose some years ago in California. A department store had complained to the police that homosexuals were using its men's room as a meeting place. The police responded by drilling a small hole in the ceiling over the enclosed stalls. A policeman then stationed himself on the floor above and peered down through the hole observing the persons using the stall for eliminatory purposes. Eventually the policeman discovered and apprehended two homosexuals who used the stall as a place to engage in forbidden sexual behavior. The California Supreme Court held the observations of the policeman to have been the result of an illegal search and ordered the conviction reversed. What made the search illegal, I believe, was that it occurred in the course of this practice, which deceived all of the persons who used the stall and who believed that they were doing in private something that was socially regarded as a private kind of thing. They were entitled, especially for this kind of activity, both to be free from observation and to have their expectations of privacy honored by the state.

There is an additional reason why the observation of certain sorts of activity is objectionable. That is because the kind of spontaneity and openness that is essential to them disappears with the presence of an observer. To see that this is so, consider a different case. Suppose I know in advance that we will be observed during intercourse. Here there is no problem of defeated reasonable expectations. But there may be injury nonetheless. For one thing, I may be unwilling or unable to communicate an intimate fact or engage in intimate behavior in the presence of an observer. In this sense I will be quite directly prevented from going forward. In addition, even if I do go ahead, the character of the experience may very well be altered. Knowing that someone is watching or listening may render what would have been an enjoyable experience unenjoyable. Or, having someone watch or listen may so alter the character of the relationship that it is simply not the same kind of relationship it was before. The presence of the observer may make spontaneity impossible. Aware of the observer, I am engaged in part in viewing or imagining what is going **on** from his or her perspective. I thus cannot lose myself as completely in the activity.

Suppose, to take still a third case, I do not know whether I am being observed or overheard, but I reasonably believe that no matter what the appearances, it is possible that I am being observed or overheard. I think it quite likely that the anxiety produced by not knowing whether one is doing an intimate act in private is often more painful and more destructive than the certain knowledge that one is being observed or overheard, despite all precautions. It is possible, for example, that one could adjust more easily and successfully in a world where one could never do things in private than one could in a world where there was always a rational likelihood that one was being deceived about the ostensible privacy in which one was acting. This is so because the worry about whether an observer was present might interfere more with the possibility of spontaneity than would the knowledge that the observer was there. If I am correct, then one of the inevitable consequences of living in a society in which sophisticated spying devices are known to exist and to be used is that it does make more rational the belief that one may be being observed or overheard no matter what the appearances. And this in turn makes engagement more difficult.

There is still an additional reason why control over intimate facts and behavior might be of appreciable importance to individuals: our social universe would be altered in fundamental and deleterious ways were that control to be surrendered or lost. This is so because one way in which we mark off and distinguish certain interpersonal relationships from other ones is in terms of the kind of intimate information and behavior that we are willing to share with other persons. One way in which we make someone a friend rather than an acquaintance is by revealing things about ourselves to that person that we do not reveal to the world at large. On this view some degree of privacy is a logically necessary condition for the existence of many of our most meaningful social relationships.

III

The fourth kind of case that I want to consider is different from the previous three. It is suggested by the example I gave earlier of all of the information that might be made routinely available to me concerning possible appointees to the job of teaching assistant. It concerns the consequences of possessing the technological capability to store an enormous amount of information about each of the individual members of a society in such a way that the information can be retrieved and presented in a rapid, efficient, and relatively inexpensive fashion. This topic—the character, uses, and dangers of data banks—is one that has received a lot of attention in recent years. I think the worries are legitimate and that the reasons for concern have been too narrowly focused.

Consider a society in which the kinds of data collected about an individual are not very different from the kinds and quantity already collected in some fashion or other in our own society. It is surprising what a large number of interactions are deemed sufficiently important to record in some way. Thus, there are, for example, records of the traffic accidents I have been in, the applications I have made for life insurance, the purchases that I have made with my Mastercharge card, the COD packages I have signed for, the schools my children are enrolled in, the telephone numbers that have been called from my telephone, and so on. Now suppose that all of this information, which is presently recorded in some written

fashion, were to be stored in some way so that it could be extracted on demand. What would result?

It is apparent that at least two different kinds of pictures of me would emerge. First, some sort of a qualitative picture of the kind of person I am would emerge. A whole lot of nontemporal facts would be made available—what kind of driver I am, how many children I have, what sorts of purchases I have made, how often my telephone is used, how many times I have been arrested and for what offenses, what diseases I have had, how much life insurance I have, and *so on*.

Second, it would also be possible to reconstruct a rough, temporal picture of how I had been living and what I had been doing with my time. Thus, there might be evidence that I visited two or three stores in a day and made purchases, that I cashed a check at the bank (and hence was there between the hours of 10 A.M. and 3 P.M.), that I ate lunch at a particular restaurant (and hence was probably there between noon and 2 P.M.), and so on. There might well be whole days for which there were no entries, and there might be many days for which the entries would give a very sketchy and incomplete picture of how I was spending my time. Still, it would be a picture that is fantastically more detailed, accurate, and complete than the one I could supply from my own memory or from my own memory as it is augmented by that of my friends. I would have to spend a substantial amount of time each day writing in my diary in order to begin to produce as complete and accurate a picture as the one that might be rendered by the storage and retrieval system I am envisaging—and even then I am doubtful that my own diary would be as accurate or as complete, unless I made it one of my major life tasks to keep accurate and detailed records for myself of everything that I did.

If we ask whether there would be anything troublesome about living in such a society, the first thing to recognize is that there are several different things that might be objectionable. First, such a scheme might make communications that were about intimate kinds of things less confidential. In order to receive welfare, life insurance, or psychiatric counseling, I may be required to supply information of a personal or confidential nature. If so, I reasonably expect that the material revealed will be known only to the recipient.

If, however, the information is stored in a data bank, it now becomes possible for the information to be disclosed to persons other than those to whom disclosure was intended. Even if access to the data is controlled so as to avoid the risks of improper access, storage of the confidential information in the data bank necessarily makes the information less confidential than it was before it was so stored.

Second, information that does not concern intimate things can get distorted in one way or another through storage. The clearest contemporary case of this kind of information is a person's arrest record. The fact that someone has been arrested is not, I think, the kind of fact that the arrestee can insist ought to be kept secret. But he or she can legitimately make two other demands about it. The person can insist that incorrect inferences not be drawn from the information; that is, the person can legitimately point out that many individuals who are arrested are never prosecuted for the alleged offense nor are they guilty of the offense for which they were arrested. He or she can, therefore, quite appropriately complain about any practice that routinely and without more being known denies employment to persons with arrest records. And if such a practice exists, then a person can legitimately complain about the increased dissemination and availability of arrest records just because of the systematic misuse of that information. The storage of arrest records in a data bank becomes objectionable not because the arrest record is intrinsically private but because the information is so regularly misused that the unavailability of the information is less of an evil than its general availability.

This does not end the matter, although this is where the discussion of data banks usually ends. Let us suppose that the information is appropriately derogatory in respect to the individual. Suppose that it is a record of arrest and conviction in circumstances that in no way suggest that the conviction was unfairly or improperly obtained. Does the individual have any sort of a claim that information of this sort not be put into the data bank? One might, of course, complain on the grounds that there was a practice of putting too much weight on the conviction. Here the argument would be similar to that just discussed. In addition, though, it might also be maintained that there are important gains that come from living in a

society in which certain kinds of derogatory information about an individual are permitted to disappear from view after a certain amount of time. What is involved is the creation of a kind of social environment that holds out to the members of the society the possibility of self-renewal and change that is often dependent upon the individual's belief that a fresh start is in fact an option that is still open. A society that is concerned to encourage persons to believe in the possibility of genuine individual redemption and that is concerned not to make the process of redemption unduly onerous or interminable might, therefore, actively discourage the development of institutions that impose permanent marks of disapprobation upon any of the individuals in the society. One of the things that I think was wrong with Hester Prynne's "A" was that it was an unremovable stain impressed upon her body. The storage of information about convictions in a data bank is simply a more contemporary method of affixing the indelible brand.

In addition, and related to some of the points I made earlier, there are independent worries about the storage of vast quantities of ostensibly innocuous material about the individual in the data bank. Suppose nothing intrinsically private is stored in the data bank; suppose nothing potentially improperly derogatory is included; and suppose what does get stored is an enormous quantity of information about the individual—information about the person and the public, largely commercial transactions that were entered into. There are many useful, efficient uses to which such a data bank might be put. Can there be any serious objections?

One thing is apparent: With such a data bank it would be possible to reconstruct a person's movements and activities more accurately and completely than the individual—or any group of individuals—could do simply from memory. As I have indicated, there would still be gaps in the picture. No one would be able to tell in detail what the individual had been doing a lot of the time, but the sketch would be a surprisingly rich and comprehensive one that is exceeded in detail in our society only by the keeping of a careful, thorough personal diary or by having someone under the surveillance of a corps of private detectives.

What distinguishes this scheme is the fact that it would make it possible to render an account of the movements and habits of every

member of the society and in so doing it might transform the society in several notable respects.

In part what is involved is the fact that every transaction in which one engages would now take on additional significance. In such a society one would be both buying a tank of gas and leaving a part of a systematic record of where one was on that particular date. One would not just be applying for life insurance; one would also be recording in a permanent way one's health on that date and a variety of other facts about oneself. No matter how innocent one's intentions and actions at any given moment, I think that an inevitable consequence of such a practice of data collection would be that persons would think more carefully before they did things that would become part of the record. Life would to this degree become less spontaneous and more measured.

More significant are the consequences of such a practice upon attitudes toward privacy in the society. If it became routine to record and have readily accessible vast quantities of information about every individual, we might come to hold the belief that the detailed inspection of any individual's behavior is a perfectly appropriate societal undertaking. We might tend to take less seriously than we do at present the idea that there are occasions upon which an individual can plausibly claim to be left alone and unobserved. We might in addition become so used to being objects of public scrutiny that we would cease to deem privacy important in any of our social relationships. As observers we might become insensitive to the legitimate claims of an individual to a sphere of life in which the individual is at present autonomous and around which he or she can erect whatever shield is wished. As the subjects of continual observation we might become forgetful of the degree to which many of the most important relationships within which we now enter depend for their existence upon the possibility of privacy.

On the other hand, if we do continue to have a high regard for privacy, both because of what it permits us to be as individuals and because of the kinds of relationships and activities it makes possible and promotes, the maintenance of a scheme of systematic data collection would necessarily get in the way. This is so for the same reason discussed earlier. Much of the value and significance of being able to do intimate things in private is impaired whenever there is a

serious lack of confidence about the privacy of the situation. No one could rationally believe that the establishment of data banks—no matter how pure the motives of those who maintain and have access to them—is calculated to enhance the confidentiality of much that is now known about each one of us. And even if only apparently innocuous material is to be stored, we could never be sure that it all was as innocuous as it seemed at the time. It is very likely, therefore, that we would go through life alert to these new, indelible consequences of everyday interactions and transactions. Just as our lives would be different from what they are now if we believed that every telephone conversation was being overheard, so our lives would be similarly affected if we believed that every transaction and application was being stored. In both cases we would go through life encumbered by a wariness and deliberateness that would make it less easy to live what we take to be the life of a free person.

IV

The foregoing constitute, I believe, a connected set of arguments for the distinctive value of privacy. While I find them persuasive, I also believe that some of them are persuasive only within the context of certain fundamental assumptions and presuppositions. And these assumptions and these presuppositions seem to be a good deal more problematic than is often supposed. What remains to be done, therefore, is to try to make them explicit so that they can then be subjected to analysis and assessment. One way to do this is to ask whether there is an alternative perspective through which a number of these issues might be considered. I believe that there is. I call it the perspective of the counterculture because it captures at least some of the significant ingredients of that point of view or way of life. In calling this alternative view the perspective of the counterculture, I do not mean to be explicating a view that was in fact held by any person or group. However, this view does provide a rationale for a number of the practices and ideals of one strain of the counterculture movement in the United States in the 1960s.

I have argued for the importance of reposing control over the disclosure or observation of intimate facts with the actor. One argument for doing so was that intimate facts about oneself—one's

fears, fantasies, jealousies, and desires—are often embarrassing if disclosed to others than those to whom we choose to disclose them. Similarly there are acts of various sorts that cause us pain or are rendered unenjoyable unless they are done alone or in the company only of those we choose to have with us.

This is a significant feature of our culture—or at least of the culture in which I grew up. What I am less sure about is the question of whether it is necessarily a desirable feature of a culture. Indeed disagreement about just this issue seems to me to be one of the major sources of tension between the counterculture and the dominant older culture of my country. The disagreement concerns both a general theory of interpersonal relationships and a view about the significance of intimate thoughts and actions. The alternative view goes something like this.

We have made ourselves vulnerable—or at least far more vulnerable than we need be—by accepting the notion that there are thoughts and actions concerning which we ought to feel ashamed or embarrassed. When we realize that everyone has fantasies, desires, worries about all sorts of supposedly terrible, wicked, and shameful things, we ought to see that they really are not things to be ashamed of at all. We regard ourselves as vulnerable because in part we think we are different, if not unique. We have sexual feelings toward our parents, and no one else has ever had such wicked feelings. But if everyone does, then the fact that others know of this fantasy is less threatening. One is less vulnerable to their disapproval and contempt.

We have made ourselves excessively vulnerable, so this alternative point of view continues, because we have accepted the idea that many things are shameful unless done in private. And there is no reason to accept that convention. Of course we are embarrassed if others watch us having sexual intercourse—just as we are embarrassed if others see us unclothed. But that is because the culture has taught us to have these attitudes and not because they are intrinsically fitting. Indeed our culture would be healthier and happier if we diminished substantially the kinds of actions that we now feel comfortable doing only in private, or the kind of thoughts we now feel comfortable disclosing only to those with whom we have special relationships. This is so for at least three reasons. In the

first place, there is simply no good reason why privacy is essential to these things. Sexual intercourse could be just as pleasurable in public (if we grew up unashamed) as is eating a good dinner in a good restaurant. Sexual intercourse is better in private only because society has told us so.

In the second place, it is clear that a change in our attitudes will make us more secure and at ease in the world. If we would be as indifferent to whether we are being watched when we have intercourse as we are to when we eat a meal, then we cannot be injured by the fact that we know others are watching us, and we cannot be injured nearly as much by even unknown observations.

In the third place, interpersonal relationships will in fact be better if there is less of a concern for privacy. After all, forthrightness, honesty, and candor are, for the most part, virtues, while hypocrisy and deceit are not. Yet this emphasis upon the maintenance of a private side to life tends to encourage hypocritical and deceitful ways of behavior. Individuals see themselves as leading dual lives—public ones and private ones. They present one view of themselves to the public—to casual friends, acquaintances, and strangers—and a different view of themselves to themselves and a few intimate associates. This way of living is hypocritical because it is, in essence, a life devoted to camouflaging the real, private self from public scrutiny. It is a dualistic, unintegrated life that renders the individuals who live it needlessly vulnerable, shame ridden, and lacking in a clear sense of self. It is to be contrasted with the more open, less guarded life of the person who has so little to fear from disclosures of self because he or she has nothing that requires hiding.

I think that this is an alternative view that deserves to be taken seriously. Any attempt to do so, moreover, should begin by considering more precisely the respects in which it departs from the more conventional view of the role of privacy maintained in the body of this essay, and the respects in which it does not. I have in mind three issues in particular that must be examined in detail before an intelligent decision can be made. The first is the question of the value that the counterculture ideal attaches to those characteristics of spontaneity and individuality that play such an important role in the more traditional view as I have described it. On at least one interpretation both views prize spontaneity and individuality equally

highly, with the counterculture seeing openness in interpersonal relationships as a better way of achieving just those ends. On another interpretation, however, autonomy, spontaneity, and individuality are replaced as values by the satisfactions that attend the recognition of the likeness of all human experience and the sameness that characterizes all interpersonal relationships. Which way of living gives one more options concerning the kind of life that one will fashion for oneself is one of the central issues to be settled.

Still another issue that would have to be explored is the question of what would be gained and what would be lost in respect to the character of interpersonal relationships. One of the main arguments for the conventional view put forward earlier is that the sharing of one's intimate thoughts and behavior is one of the primary media through which close, meaningful interpersonal relationships are created, nourished, and confirmed. One thing that goes to define a relationship of close friendship is that the friends are willing to share truths about themselves with each other that they are unprepared to reveal to the world at large. One thing that helps to define and sustain a sexual love relationship is the willingness of the parties to share sexual intimacies with each other that they are unprepared to share with the world at large. If this makes sense, either as a conceptual or as an empirical truth, then perhaps acceptance of the counterculture ideal would mean that these kinds of relationships were either no longer possible or less likely. Or perhaps the conventional view is equally unsatisfactory here, too. Perhaps friendship and love both can and ought to depend upon some less proprietary, commercial conception of the exchange of commodities. Perhaps this view of intimate interpersonal relationships is as badly in need of alteration as is the attendant conception of the self.

Finally, we would want to examine more closely some other features of the counterculture ideal. Even if we no longer thought it important to mark off and distinguish our close friends from strangers (or even if we could still do that, but in some other way), might not the counterculture ideal of openness and honesty in all interpersonal relationships make ordinary social interaction vastly more complex and time-consuming than it now is—so much so, in fact, that these interactions, rather than the other tasks of living, would

become the focus of our waking hours?

These are among the central issues that require continued exploration. They are certainly among the issues that the fully developed theory of privacy, its value and its place within the law, must confront and not settle by way of assumption and presupposition.