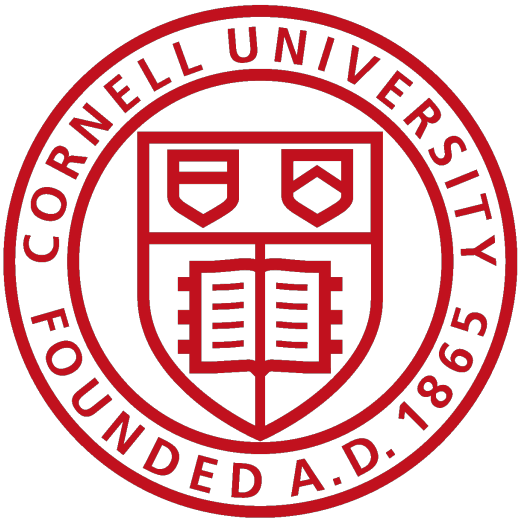
How Technology Undermined and Clarified Privacy: Camera to Internet



Ishaan Anand Jhaveri

Advisor: Dr. Fred B. Schneider

Honors Thesis

Submitted in Partial Fulfillment of the Requirements for the Computer Science Honors Program

Cornell University

Ithaca, New York

May 23, 2017

Abstract

Today the Internet "threatens privacy". But it is difficult to define what constitutes privacy. We attempt to do so by creating a lens through which to think about privacy implications of any new technology. We conceptualize privacy in terms of technology's relationship with it. We discuss privacy implications of existing technologies, namely the camera, the telephone and Global Positioning System (GPS). We examine what elements of these technologies disrupted privacy enough to trigger legal redress, attention from privacy scholars or public response. We then use our lens to comment briefly upon the changing meaning of privacy. Our lens looks at the way new technologies (1) create new types of information, (2) increase the fidelity of captured information, (3) increase the dissemination of information, (4) lower the standard of notice or consent to authorize the capture of information, (5) manipulate the integrity of information and (6) increase the prevalence of information. It further isolates threats to privacy by looking at phenomena that have threatened privacy in the past.

Acknowledgements

The fledgling idea that became this thesis began forming over a few evenings in the summer of 2016. I was working in the tech industry in Seattle, Washington at the time, putting many of the skills I had learnt in the first three years of my undergraduate education to work. I would spend my evenings reflecting on the day, on my work, on the positive and negative impact of my work on society. These thoughts began taking a more definitive shape when my friends Austin, Jack and Sumer started telling me about the theses they were planning on writing over the upcoming academic year, and I began to conceptualize this idea as a thesis I could write. I thank them for being reliable sounding boards for my early ideas. I decided then to spend the last year of my undergraduate education commenting on some of the ways the skills I was accruing affected society, particularly how technology informs privacy norms. The first person that encouraged me to take this idea forward and write a formal paper about it was my academic advisor, Professor Dexter Kozen. I owe him thanks for this. Through his direction I found Professors Karen Levy and Fred Schneider, who had an interest in the subject I wanted to write about. I am indebted to both of them for their expertise and guidance.

To Professor Levy, I owe much of the approach of this paper. The foundational readings she gave me on Science and Technology studies, a field I was new to, helped me understand the standard and ilk of scholarship expected of me in this endeavor. Our early conversations on the reactions of privacy scholars to technologies in the past taught me what to look for in my research into each of the technologies I discuss in this thesis. Since both Professor Schneider and I were newbies in Science and Technology studies, her comments on later versions of the thesis helped add an extra degree of legitimacy to my claims. When my research would hit a wall, she would always greet me with an open door and a smiling face, and assure me that my work was interesting even to people like herself who have studied it much longer than I have.

To Professor Schneider, I owe the entirety of this project. Had he not agreed to advise me and take me under his wing, the idea would have lived and died in Seattle and never persevered to become the complete twenty-five thousand word essay I can now proudly say it is. I proposed this idea as a non-technical look at an area of Computer Science, a

journey I was unfamiliar with; he not only agreed to embark upon the journey with me, but, time and again, steered me back on course when I lost my way. It is a testament to his strong work ethic and dedication to this project that he never took more than a day or two to read and comment upon any amount of drafts or material I would deluge him with, frequently met with me for hours at a time, long after the sun went down, and promptly responded to all my questions and clarifications, no matter what time of day or night they arose. He did all of this while balancing his considerable other responsibilities as a professor, department chair, recent inductee into the American Academy of Arts & Sciences and all round distinguished academic. His declaration in our very first meeting that "the dust hasn't yet settled with the Internet" is responsible for the deep historical reach of this thesis that has widened the scope of my original idea more than I could have ever anticipated. His suggestion to cast my ideas as a lens that can be applied to any new technology gave the idea the functional thrust it lacked in its original form, when it was just a series of meditations on technology and privacy. He always encouraged me to bounce all manner of ideas off him, and always had advice to give when I sought it, whether about this project or about what I should do with my beard. We would sometimes joke that I owe him a cent for every obsolete word he removed from my drafts. I probably owe him a thousand dollars.

When the going got hard on this project and I was strapped for time, I found myself often in need of people to cover my shifts at the Temple of Zeus café. I thank all of the people that covered for me in these times, particularly my sister, Mana and my friend Susie. I thank my friends Drew and Emily for proofreading parts of my work. I thank my friend Rayaan for suggesting examples of privacy infringements for me to look further into. I thank my roommates at 111 Osmun Place and my friends in and out of Cornell for their support through this project. Finally, no work of mine would be complete without an acknowledgement to my parents Anand and Saloni Jhaveri for their love and encouragement through all of my endeavors.

Table of Contents

1 Abbreviations

1. CALEA – Communications Assistance for Law Enforcement Act
2. DEA – Drug Enforcement Administration
3. DOITs – dimensions of information technology
4. EU – European Union
5. FCC – Federal Communications Commission
6. GPS – Global Positioning System
7. GIC - Group Insurance Commission
8. LC – Lord Chancellor
9. MIT – Massachusetts Institute of Technology
10. PT&T – Pacific Telegraph and Telephone Company

2 Figures

1. Telephone Proliferation Picture. Page 27. Taken from 30, page 90.

3 Introduction

On March 11, 2015, Intelligence Squared US hosted a debate that centered around the question "Should the U.S. should adopt the 'Right to be Forgotten' online?" [4]. The Right to be Forgotten gives EU citizens "the right—under certain conditions—to ask search engines to remove links with personal information about them" [1]. In this debate, Eric Posner, a Law Professor at the University of Chicago arguing for the motion said,

> I want you to imagine back then in 1990 that an academic—a kooky academic like me came up with the following proposal, '… we should … record everything that everybody does, put it onto a searchable database, and make this database available to everybody in the world'. We would have been laughed out of the room—'What a ridiculous proposal, what a tremendous invasion of people's privacy.' But, of course, this is what's happened … because of the development of the Internet. [Video at 1, 24-26 minutes]

The power of publicly available records of "everything that everybody does" cannot be overstated. In the 1990s, the Massachusetts Group Insurance Commission (GIC) released "anonymized" data on state employees' hospital visits to help researchers interested in healthcare. The data was thought to be anonymous because unique identifiers like patient name, social security number, and others were removed from the publically available records. William Weld, the Governor of Massachusetts at the time, was publicly in favor of the release, and he assured Massachusetts' residents that "GIC had protected patient privacy by deleting [unique] identifiers" [8] In a bid to show the governor the limits of "anonymization," Latanya Sweeney a graduate student in Computer Science and Electrical Engineering at MIT attempted to prove she could find Governor Weld's own hospital records:

> She knew that Governor Weld resided in Cambridge, Massachusetts, a city of 54,000 residents and seven ZIP codes. For twenty dollars, she purchased the complete voter rolls from the city of Cambridge, a database containing, among other things, the name, address, ZIP code, birth date, and sex of every voter. By combining this data with the GIC records, Sweeney found Governor Weld with ease. Only six people in Cambridge shared his birth date, only three of them men, and of them, only he lived in his ZIP code. [8]

Though identifiers like name and social security number were excluded from the

hospital-visit data, patient birth date, sex, and ZIP code were not. This allowed Dr. Sweeney to identify the governor's own hospital visit record with ease, gleaning uniquely identifiable information about an individual from apparently "anonymized" public data.

Such sentiments voiced by privacy advocates like Professor Eric Posner (or the fact that the debate in which he voiced these sentiments was even organized) and the uses of this immense volume of publically available information as demonstrated by scholars like Dr. Sweeney raise questions about the Internet and society today. The ease with which data about one's opinions, location, purchasing habits, and even DNA is collected and disseminated raises questions like: "who has a right to collect this information" and "what harm can this information cause to the people to whom it pertains." Conversations about use and effects of information made available by the Internet are usually conducted under the banner of "threats to privacy." People talk about the Right to Privacy and about the Internet's infringing upon one's privacy. Yet the difficulty in having this discussion is that privacy is a nebulous concept that escapes simple definition. As Alan Westin says, "[f]ew values so fundamental to society as privacy have been left so undefined in social theory" [47]. The challenge of discussing "privacy implications" of the Internet (or of technology at large), then, is that we do not have a concrete definition.

This thesis attempts to address this challenge by suggesting a lens through which to view privacy-implications of any new information and communication technology. We conceptualize privacy in terms of technology's relationship with it. In aid of this, we discuss privacy implications of existing technologies: the camera, the telephone and Global Positioning System (GPS). We do not claim that technology is the sole lens through which all conversations about privacy should be had, but we will attempt to create a model that facilitates conversations about privacy with respect to technology at large and specific technologies, both new and existing. Our goal is to understand what elements of a new technology are likely to so disrupt privacy that legal redress, attention from privacy scholars, or public response results. We present this lens as a basis to predict which new technologies or technological practices are likely to merit scrutiny for legal protections in the name of privacy. A functional use of this lens is to discern the changing meaning of the concept of privacy.

Section 4 lays out our approach to creating this lens, and summarizes the two components of it, namely dimensions of information technology and privacy canaries. Sections 5 and 6 discuss these in greater detail. Section 7 examines the effect of the camera, telephone and GPS on conceptions of privacy, using our lens. Section 8 discusses the applications of our lens to conversations about the Internet and privacy and the extent to which our lens can be used as a response to work by privacy scholars Solove and Calo. Finally, Section 9 analyzes our lens critically.

4 Approach to Creating the Lens

The initial goal of the project that ultimately became this thesis was to discuss the implications of the Internet on privacy. We wanted to understand why the Internet is widely castigated as a tool that enables people to know too many intimate details about each other—that allows governments to spy on their people. We wanted to understand, at its very core, what elements of the Internet had triggered discussions about privacy—what it was about the Internet and what it was about privacy that caused them to be so intertwined.

Heeding Stanford Communications Professor Angèle Christin's suggestion that "there is a relative amnesia about the continuities that exist between the Big Data revolution and historical precedents involving similar technological, economic and political dilemmas," [20] we reasoned that the Internet couldn't have been the first technology that received attention from privacy advocates. So to understand the character of this attention, we looked at attention from privacy advocates to technologies in the past. Past technologies might help identify elements shared by various technologies.

The question now became which technologies to choose, and what to define as privacy when examining how they affected privacy. Nissenbaum's work helps us with the latter. Nissenbaum recognizes that privacy is very subjective to context when she puts forth the theory of contextual integrity:

> Contextual integrity is a philosophical account of privacy in terms of the transfer of personal information. It is not proposed as a full definition of privacy, but as a normative model, or framework, for evaluating the flow of information between agents (individuals and other entities), with a particular emphasis on explaining why certain patterns of flow provoke public outcry in the name of privacy (and why some do not). [10]

Her theory offers a formal system of mapping information flow in different contexts to determine whether a particular flow of information is a privacy violation. For example,

> … in the context of a job interview for the position of bank manager in the present-day United States, information about applicants' marital status is inappropriate, but it is appropriate in the context of dating (or courtship). Because information type is so salient an influence on people's

> judgments that a violation has occurred, earlier accounts of contextual integrity had posited norms of appropriateness as distinct from norms of transmission.

Though Nissenbaum states that defining privacy as the control of flow of information does not fully encompass privacy, we believe it is a good starting point. Technology is immediately relevant to this definition, because technology creates new types of information and new channels for the flow of information. It therefore makes controlling information more difficult.

Nissenbaum's definition helps us isolate what aspects of an information technology disrupt privacy. These aspects form the first part of our lens, dimensions of information technology (DOITs). To identify DOITs, we decided to look at prior technologies that have affected privacy. Certain technologies select themselves, both as precursors to the Internet and as technologies that were given attention by privacy advocates. We also wanted to choose technologies that are representative of a wide temporal scale. So we chose the portable camera popularized in the 1880s and 1890s, the telephone, which spread widely in the 1920s, and GPS, which was invented in the 1960s for the military and commercially available in the 1990s.

Searching for DOITs isn't always easy. Though examining whether a new technology undermines control of the flow of personal information is a good approach, sometimes understanding what information is personal or what constitutes control can be difficult. Therefore, it is helpful to understand what has always been valued as private in society. Hence, we propose *privacy canaries* as the second part of our lens. We define privacy canaries as cases, writings, laws, or situations that demonstrate why it is valuable for certain information to be kept private. These can be considered precedents to the laws and reactions from privacy scholars to the technologies we discuss in the ensuing sections. We discuss privacy canaries in Section 6.

Thus our lens is a set of DOITs and privacy canaries that can be used to ask questions about how a new technology might affect privacy. This lens is particularly useful when laws are enacted to prevent a technology from infringing upon people's privacy.

5 Dimensions of Information Technology (DOITs)

In looking for situations having privacy implications, we seek situations that involve controlling the flow of information. So we are concerned with means by which information is collected, means by which information is distributed, and uses of that information. New technologies create the ability to collect new kinds of information about people and to disseminate it both in new ways and to new communities. New kinds of information can be put to new uses. The camera created, for the first time, the ability to collect accurate, instant, visual information on a large scale about people, just as the microphone first allowed audio information to be collected. The Internet created a new way of distributing any kind of information about anyone.

Technology allows reality to be recorded in novel ways, creating novel types of information. It also increases the quantity of existing types of information that is collected and used. To characterize these changes, we propose the following basis for determining whether a new technology should be scrutinized for legal protections in the name of privacy.

We contend that a new technology might spark changes in privacy law only when it increases or changes one or more of these:

5.1 What *type* of information can be collected

Before the invention of the microphone, there was no such thing as collectible audio information about someone. One could be overheard, but not recorded. A recording constitutes a new type of information. Now that this information can be captured, the person or group to whom this information pertains might have an interest in controlling its flow. Laws giving one the right to control this new kind of information should be expected.

5.2 The *fidelity* of information

The camera increased the accuracy of recorded visual information. Portraits and paintings offered the artists' (or subject's) view of reality, allowing the artist to highlight some details while hiding others; the camera delivers increased detail. As camera technology developed, the scope and resolution of images increased, augmenting the

accuracy of information in pictures. Advances in technology can increase the fidelity of recorded information about someone, and thus capture more personal details. The more detail that is collected about someone, the more powerful that information can be. Now people will seek greater control, and legal redress is one approach.

5.3 The *dissemination* of information

There was a time when the subject of a photograph had full control over who could see that photograph (The person who took or possessed the photograph probably had even more; not necessarily the subject). Physical control over the printed photo sufficed, because there were no copies anywhere else. Today, as soon as a photo is posted anywhere, the subject loses control over who can see it. Technological developments facilitated spread of information. Facebook is the canonical example. As soon as one's photo appears on Facebook, there is no telling how far and wide copies of that photo can travel. The more widely disseminated that information is, the harder it is to control. Law might be needed to regulate the ability to spread information across an unprecedented scale.

5.4 The *standard of notice or consent* to authorize the capture of information about a person or group

Before microphones were invented, people could control what information they divulged in speech by controlling with whom they chose to speak. But with the advent of the microphone, recordings can be made with or without consent. Similarly when the portable camera was invented, photographers could hide and photograph people without the latter's knowledge. The quick, unobtrusive, convenient nature of many technologies enables information to be captured without a subject's explicit consent.

5.5 The *integrity* of information

This may appear similar to the fidelity of information, but there is a subtle difference. Before photo editing or the ability to cut different audio clips together, when one consented to a being in a photo or a recording, it was with the belief that the information about them wouldn't be taken out of the context they presented it in. Technology makes it

increasingly easy to alter information, presenting it in a form that the subject of that information does not have control over, and may not want to broadcast. This is different from fidelity because altering information may not necessarily increase detail, but can still alter context.

5.6 The *prevalence* of information

Paper records of peoples' transactions with businesses have existed from time immemorial, as have arrest records. However, before records were digitized, this information was often destroyed, because recordkeeping was expensive. Records were also inconvenient to find, a form of "security by obscurity"[1]. Information has become cheap to store with the advent of data centers and easy to access with the advent of search engines. These inventions make records of arrests easy to find. Even if records are "sealed", as certain states allow by petition, [27] though the actual record would be unobtainable, articles related to the incident in newspapers are easily uncovered by search engines. Technology makes information persist longer, increasing the burden of controlling its flow.

Technology allows information to be used for a wider variety of purposes. The rest of this thesis explains how these six dimensions emerged from examining privacy related reactions to the camera, telephone, and GPS. We examine actual legal responses, attention from privacy advocates and scholars, and reactions of the general public.

[1] "Security through obscurity" is outside the scope of this work, but one can look here for more information about it:
http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=4192&context=californialawreview

6 Privacy Canaries

Understanding cultural and legal norms related to privacy throughout history is key to understanding the disruptions caused by technology.

6.1 Philosophical Writings about the Value of Privacy

For the most part, "Few philosophers would argue that privacy is a 'natural' right or that the intrinsic nature of privacy establishes it as a legal right." [41] However, there have been notable historical writings about the value of what we today call privacy.

Book I of Aristotle's *Politics* is entirely devoted to establishing the difference between the *polis* or public sphere where an individual is a citizen before the government and can engage in the politics of the society and the *oikos* or private, family sphere, where one can formulate independent, individual opinions [65]. Other philosophers, notably Immanuel Kant and John Stuart Mill, echo this idea in their writings. In *On Liberty*, John Stuart Mill contends that there is a sphere in which society can dictate how an individual should conduct him or herself—the public sphere where one's actions affect others—but there should also be a private sphere, where society should not have a right to dictate what is best for an individual or what behaviors an individual can or cannot engage if those behaviors do not interfere with anyone else's liberty or well-being. According to Mill, this sphere is essential for independence of thought. He agrees that the public can claim to know what is best for an individual within the class of behaviors that can harms others, but outside of this class of behaviors, only the individual knows best what is best for himself or herself—for the public to try and monitor an individual in this realm is an infringement on what we would today call privacy. Kant similarly advocates for every individual to exist in the capacity of their formal role in society—be it citizen, leader or government worker—but also in a private capacity. He writes,

> Thus it would be ruinous for an officer in service to debate about the suitability or utility of a command given to him by his superior; he must obey. But the right to make remarks on errors in the military service and to lay them before the public for judgment cannot equitably be refused him as a scholar. [36]

Kant argues that no individual should be denied the right to be a "scholar", the right to form their own opinions independently of what is expected of them in any official or public capacity.

These philosophers are not talking about the flow of information, secrecy, the right to be let alone, or anything that is a possible definition of privacy. But their writings make a strong cases for why all of these things should be protected. They emphasize the importance of protecting the private realm, in order to protect the ability to exercise free thought and, thus, enjoy freedom. They suggest a value of privacy. The United States First Amendment, which protects freedom of speech and freedom of the press, shows that society today still values free thought and expression. In our examination of reactions to technological change, these writings guide what to look for—changes that mitigate an individual's ability to enjoy this private realm or form these private opinions. As we later discuss, we conceptualized the DOITs that, if changed, would mitigate these abilities.

6.2 Libel, Defamation, and Slander

"Early in the middle ages[,] reputation was protected in England by the combined secular and spiritual authorities" [59, p.546-7]. *Lex Salica*, the ancient Frankish civil law code compiled around 500 AD by the first Frankish King, listed penalties for such infractions as calling men "wolf" or "hare", or insinuating unchaste things about women. Such protection of reputation prompted King Alfred in 9th century England to rule that slanderers should have their tongues cut out. "Meanwhile the Church punished defamation as a sin" [59, p. 550]. By Church Law and eventually under the king, defamation was considered personal injury and punished as such: "Early in the seventeenth century it was stated that 'where words spoken do tend to the infamy, discredit or disgrace of the party, there the words shall be actionable'".

The extent to which both the Church and Crown were prepared to protect reputation was further tested by the invention of the printing press. "In early times libels must have been comparatively rare and harmless: rare, because few could write, harmless, because few could read" [59, p. 561]. This changed with the invention of the printing press, with "this new method of diffusion of ideas" [59, p. 561]. The Crown feared the spread of libelous publications: "censorship became part of the royal

prerogative, and the printing of unlicensed works was visited with the most severe punishment" [59, p. 561]. From here, laws specifically outlawing libel, slander and defamation were enacted:

> The first comprehended defamatory and injurious statements which were made in a public manner (*convicium contra bonos mores*). The essence of the offen[s]e in this case lay in the unwarrantable public proclamation, in the contumely which was offered to a man before his fellow citizens. In such cases the truth of the statements was no justification for the unnecessarily public and insulting manner in which they had been made. The second head included defamatory statements which were made in private. Since the offen[s]e in this case lay in the imputation itself, not in the manner its publication, the truth was a complete defen[s]e; for no man had a right to demand protection for a false reputation. The law thus aimed to give ample scope for the discussion of personal character, while it forbade the infliction of needless insult and pain… Imperial legislation subsequently established supplementary criminal actions under which certain kinds of defamation were punished with great severity. These were the *libelli famosi*[,] particularly epigrams and pasquinades, which, being their nature anonymous and scurrilous, were regarded peculiarly dangerous and were visited with severe punishment, whether true or false. The unnecessarily public and offensive manner of their publication (they were general scattered about the streets) precluded justification. [59, p. 564]

The "crime was not based on the form of the publication, but upon the character of the matter published, the extent of its diffusion, and its anonymous nature" [59, p.564-5]. These laws show that medieval English society valued privacy as a way of protecting reputation. Injurious statements about people were punished as libel if they were made publicly, whether they were true or not. Injurious statements made privately however, were not punished if they were true. The law suggests strongly that poor character traits ought to be called out, but not publicly. Without using the term privacy, this law incorporated an appreciation for an individual's right for the public not to know certain things about them. That the laws were made stricter after the invention of the printing press informs our lens. Printed, as opposed to written text, was a new form of information; the printing press allowed material to be reproduced easily, facilitating dissemination; finally "the anonymous nature" of the publication meant that the person mentioned in the printed information hadn't given consent to its publication.

In the United States, laws related to defamation were notably different. In 1735, John Peter Zenger, editor of *New York Weekly Journal*, was brought to trial on charges of printing false and seditious statements about British officials [53]. He was eventually acquitted on grounds that he had not printed anything false, and this set the legal precedent in the United States that *truth* is a defense against charges of libel. In the United States, veracity of information would usually trump the means by which it is obtained.

Though this was how the law was structured, reputation was still important in society. In an 1890 article written in response to the growing tendency of newspapers to print "gossip" about people, prominent social commentator E.L. Godkin laments,

> …when anyone wishes seriously to damage reputation nowadays, he inevitably seeks to put it in a newspaper, as the channel through which he can obtain most publicity, and make his attack most seriously felt. [32]

Godkin goes on to argue that there is a much more damaging character to gossip when it is written rather than simply spoken, for in this form it transcends ones private social circle and becomes "known hundreds or thousands [of] away from his place of abode." [32] This sentiment is similar to the one evidenced by the law in England. In fact Godkin even pens the term "right to privacy", in this article—he requests the public at large to respect this right by not printing personal information about one another in newspapers. That his article was in response to newspapers' tendency to widely disseminate private information informs our lens.

6.3 Breach of Confidence

In England, there arose the Breach of Confidence tort: in 1849 the High Court of Chancery awarded a plaintiff, Prince Albert, an injunction, restraining the defendant, Strange, from publishing a catalogue describing Prince Albert's etchings. Strange had obtained these etchings from a printer. Prince Albert objected to the manner in which Strange had obtained the etchings and his publishing a catalogue of them without the Prince's consent. Lord Cottenham LC noted "this case by no means depends solely upon the question of property, for a breach of trust, confidence, or contract, would of itself entitle the plaintiff to an injunction" [62]. The resulting Breach of Confidence tort in

English law provides that one who misuses "information provided in circumstances importing an obligation of confidence" and discloses that information without the consent of the person or group who gave it to them shall be punished accordingly [13].

Note, the focus of the legal literature in England was on the means of discovering information and consequences of disclosing that information. The Breach of Confidence tort protects something that could be called privacy. It implies that, according to law, people have a right to control information about them, or to control material created by them from use in ways they haven't consented. It punishes wrongful dissemination of information. This law supports our inclusion of consent to information's use, and dissemination of information as DOITs in our lens.

This tort existed in England around 1890 when the camera was invented, but no such tort, or similar law existed at that time in the United States.

6.4 Eavesdropping

Under the Common Law in England, "*Eavesdroppers,* or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance and presentable at the court-leet, or are indictable at the sessions and punishable by fine and finding sureties for their good behavior" [12, p. 2362-3]. However, there are no modern instances of a prosecution or indictment in England for eavesdropping per se.

In the United States, this definition was cited in an 1859 case in Tennessee where the defendant, Fielding Pennington, was tried for eavesdropping on the proceedings of a jury in another trial. The State contested that the defendant "unlawfully and stealthily did approach and come near to the room where the jurors … were then and there assembled … for the purpose of listening to, and overhearing what was then and there said … and was then and there guilty of the crime of eaves-dropping" [34, p. 225]. Though the Circuit Court of Knoxville quashed the charge, ruling that it was not an indictable offense, the Supreme Court of Tennessee overturned the ruling in 1861, citing the definition of eavesdropping in the Common Law above. This was the first use of the term "eavesdropping" in a US court ruling. This law shows that listening to someone without

their knowledge (and therefore consent) was frowned upon by the law, long before many technologies of today were invented.

6.5 Search and Seizure

It is possible to read the Fourth Amendment as a legislative protection of the private sphere, as discussed by philosophers above.

> The Fourth Amendment was a response to the British writs of assistance, which empowered officers of the Crown to search "wherever they suspected uncustomed goods to be" and to "break open any receptacle or package falling under their suspecting eye" (Lassen 1937, p. 54). In framing the laws of the new nation, the founders sought to avoid creating such unrestricted governmental powers. [24]

The Fourth Amendment states:

> 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. [55]

This legislation proves to be influential and increasingly relevant to discussions about privacy, as we see in later sections.

6.6 Reading Mail

In 1710, the British government took over the colonial American mail service and passed the Post Office Act: a law in the colonies forbidding the "open[ing], detain[ing], delay" of "any letter or letters, packet or packets" without the approval of the Secretary of State, similar to a law that existed at the time in England [46, p. 8]. This English law was frequently violated by the British colonists to spy on revolutionaries. Thus they "had a visceral understanding of the importance of postal privacy" [24, p. 145]. Once they had control of the law of the land, they wanted to ensure postal privacy for all, because of how much they grew to value it. Thus, in the Postal Act of 1792, they outlawed reading of mail by postal officials unless the mail was undeliverable. Subsequently, Congress passed the Postal Act of 1825, which prohibited reading another person's mail. In 1878,

the Supreme Court even ruled that no government official of any rank could open anyone's First Class mail without a warrant. In delivering the opinion of the court, Justice Field declared "no law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution" [29].

This is an interesting precursor to our discussion of the development of privacy law as reactions to new technologies.

> This example illustrates that privacy is not just found but constructed. By erecting a legal structure to protect the privacy of letters, our society shaped the practices of letter writing and using the postal system. It occurred because of the desire to make privacy an integral part of these practices rather than to preserve the status quo. [47]

This, like the printing press, is a case where the value lawmakers place on something that could be called privacy is seen by their reaction to changing circumstances. Their construction of privacy sheds light on its meaning. This is exactly what we are trying to do with technology. This case also informs our lens: protecting information from interception is a form of controlling dissemination.

These privacy canaries show some of what society protects as private. In the next section, we will examine how technological change has created situations where things viewed as private are infringed. The reaction of lawmakers show us whether they chose, in those moments, to continue to protect what was historically private against infringement by technology, or whether they chose to sacrifice past privacy norms in order to embrace technology-driven societal change. Our lens guides us in that conversation, since it pinpoints the nature of technological change.

7 Technologies

7.1 Eastman's Portable Camera and Talbot's Halftone Embolden Warren and Brandeis

7.1.1 Technological Changes

Louis-Jaques-Mandé Daguerre's daguerreotype camera, distributed worldwide starting in 1839, was the first widely available means of photography. It is estimated that by 1853, three million daguerreotype photographs were being taken annually in the United States. These photographs were expensive to take. The equipment needed was bulky and complicated to use. So access to daguerreotype photography was largely restricted to professional artists, scientists, and wealthy families. Most daguerreotype photos were taken in studios. To visit such a studio required time and money. A subject had to hold a motionless pose for twenty seconds to a minute, thereby limiting the types of scenes that could be captured. Motion could not be captured. Moreover, it was difficult to take a photo without the subject's consent. As Calo notes, "you not only had to give your consent, you had to cooperate a lot." [54]

Though the first picture in a newspaper was in 1842 in *The Illustrated London News* (an artist's impression of the attempted assassination of Queen Victoria), pictures in the mid-nineteenth century were rarely seen in newsprint. Daguerreotypes were not reproduced widely in newsprint because there was no method to mechanically reproduce photographs at the time. In order to print pictures,

> Artists would make a sketch of the scene, followed by a more detailed drawing. The drawing would be copied, sometimes in reverse, onto a smooth block of wood. A craftsman would cut away [the entire] surface except the lines to be printed. In these pictures shadows were represented by many small separate strokes… The finished block would then be pressed into clay, making an impression of the image. Molten type metal was then poured onto the clay making a cast. This cast plate was used in the "letterpress" printing process where raised areas of metal carry the ink. [49]

Though the daguerreotype slightly sped up the initial part of this process by replacing the artist's sketch with a photograph, there was no technology to reproduce the daguerreotype photograph in original form. If it was reproduced, then much of its original detail would be lost, because "the wood engraving and printing processes of the time could render only solid backs and whites; the intermediate shades of grey found in a

photograph could not be reproduced" [49]. Thus, each daguerreotype photo was an individual entity that had to be physically transported in order to be disseminated.

Two innovations would change this state of photography forever: George Eastman's portable camera and William Fox Talbot's halftone printing technique. In 1888, George Eastman invented "dry, transparent, and flexible, photographic film" and portable cameras that could use the new film [2]. "'You press the button, we do the rest' promised Eastman's advertising slogan." [2] He designed the camera specifically to be simple, small enough to fit in one's hand and cheap. For twenty-five dollars, one could buy the camera pre-loaded with a hundred-exposure roll of film [31]. When one had used up the entire roll, one could send the camera to Eastman's Rochester factory, and for ten dollars get all the photographs developed and a new roll of film. This camera enabled amateurs to take photographs. They could afford the equipment, and they didn't need to understand a complicated process of development or to use a studio in order to create a photograph. People devoid of artistic skill could take and collect photos, and they did so on a large scale. By 1896, 100,000 Kodak portable cameras had been produced, and demand had pushed photographic film production up to a rate of 400 miles per month. [11, p. 255]

In 1852, William Fox Talbot invented halftone printing. This technique used dots to represent gradients in color. The spacing, size and density of the dots were used to fill in the intermediate shades of grey that existed in photographs but couldn't be reproduced in print. Throughout the 1870s and 1880s, various printers used and improved Talbot's halftone technique until it evolved into a technique that enabled the quick, easy and cheap reproduction of photographs in newspapers.

The result of these two innovations was that, by the turn of the century, photographs widely replaced artists' renderings in newspapers, and a third of American households possessed a portable camera [3].

7.1.2 Discussion with respect to lens

Type. Though images were not new, the portable camera vastly increased the types of scenes that could be captured by photography. It enabled the capture of motion and life outside the studio. It allowed creation of a visual record of people's activities in a wide

variety of situations, documenting things that could never have been documented before. The scale of capture for this information increased unprecedentedly: recall that only three million daguerreotype photographs were captured per year in 1853, but over one hundred million Kodak photographs were captured *per month* (if it is assumed that one mile of film can produce roughly 250,000 individual photographs, 400 miles produces over one hundred million photographs) by 1896. That photographs could be printed easily in newspapers meant that photography and photojournalism emerged as forms of news in the 1890s. This became a popular new way of conveying information to the public.

Fidelity. Eastman's film was the beginning of innovations in photography that increased the resolution of captured images. Pictures from the Kodak camera were more discernible than sketches, portraits, or daguerreotype pictures. Thus, the portable camera increased the fidelity of whatever limited visual information already did exist.

Notice or Consent. Eastman's camera allowed photographs to be taken covertly without giving a subject notice or seeking the subject's consent—which would never have been possible with the daguerreotype.

Dissemination and Prevalence. Godkin had already lamented the potential for the widespread dissemination of personal information in newspapers. Halftone printing technique allowed photographs, a potentially new form of personal information, to be included in newspapers and, consequently, distributed far and wide. This easy copying and wide distribution also increased the prevalence of information, since once in newsprint, the information was recorded and could be referred to thereafter.

Integrity. Cameras capture specific snapshots of reality that often do not represent the entire situation. Consequently, the visual information they record can present a seemingly alternate view of reality. This is especially true when photographs are printed alongside text and in specific contexts in specific articles or journals—the innovations in the late nineteenth century increased the potential for these situations.

7.1.3 Reactions and discussion of the meaning of privacy

The public in the United States and England saw the potential for innovations in photography to tarnish people's reputations. In the United States, the phenomenon of the so-called "Kodak Fiend" arose. An 1890 *Hawaiian Gazette* editorial had the following to say about the prevalence of portable cameras:

> Have you seen the Kodak fiend? Well, he has seen you. He caught your expression yesterday while you were in recently talking at the Post Office. He has taken you at a disadvantage and transfixed your uncouth position and passed it on to be laughed at by friend and foe alike. His click is heard on every hand. He is merciless and omnipresent and has as little conscience and respect for proprieties as the verist hoodlum. [35]

In England, *The Weekly Times and Echo* wrote in 1893:

> Several decent young men, I hear are forming a Vigilance Association for the purpose of thrashing the cads with cameras who go about at seaside places taking snapshots of ladies emerging from the deep. [45, p. 61]

The public recognized this new type of information and the detail it could capture. The editorials above show that many people were enraged by the potential for covert photography without a subject's notice or consent, and the subsequent dissemination of this photography.

Scholars reacted, too. Two years after Eastman invented rolled photographic film, law scholars Samuel Warren and Louis Brandeis published an article titled "The Right to Privacy" in the Harvard Law Review's December 1890 issue advocating for a "right to be let alone". They argued for a constitutionally recognized right to privacy, writing: "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.'" They felt that publication of one's "manuscripts or works of art" should not be allowed without one's consent, and thereby felt that everyone should have a right to be let alone. Clearly they were reacting to the camera's ability to capture information that could not have been captured before its invention, and the halftone innovation's ability to broadcast it in newsprint. In fact, some sources allege that both Warren and Brandeis'

personal lives were often reported in Boston's *The Saturday Evening Gazette*, to both of their displeasure. [45, p. 11] It is believed that E.L. Godkin's article lamenting the printed dissemination of gossip that was discussed previously (written in July 1890, six months before their Harvard Law Review article) had an influence on them—it took the changes spurred by these innovations for them to write their own article underscoring the importance of reputation, and a right to be let alone that would protect it.

Warren and Brandeis reasoned that a "right to be let alone" was not adequately protected under existing law in the United States at the time—new law was needed. "[O]ur system, unlike the Roman law, does not afford a remedy even for mental suffering which results from mere contumely and insult, but from an intentional and unwarranted violation of the 'honor' of another", they claim. Warren and Brandeis had realized that, though copyright law did protect the privacy of what one wrote, painted, or sculpted (etc.) if one chose not to publish, this law could no longer protect the use of one's work once it had been published. "[C]opyright law that could protect individual letters had become inadequate/obsolete with the rapidly evolving technology that could disgorge one's privacy without stealing or copying any tangible items" [56]. Property law fell short in protecting how a photograph of someone is used, because in taking a photograph of someone, no property is physically divested. In their seminal article, they cited *Prince Albert v. Strange*, explaining how a defendant had wrongfully acquired the prince's etchings [52]. As discussed previously, the court gave an injunction to the defendant to refrain from publishing the etchings without the prince's consent, because such a publication constituted a "breach of trust, confidence, or contract", and that prevented the defendant from having the right to put that information (the Prince's etchings) to any use. Warren and Brandeis agreed with this.

Physical and Intellectual Copyright Law had provided a right to prevent publication of one's intellectual property (and, by extension, personal information). But this law didn't address the use of one's property after publication. In contrast, with photography, one's property or "information" could be used in different ways—even after publication—and potentially in ways the subject of a photograph didn't consent at the time of the photograph.

Warren and Brandeis thus set forth four harms from privacy invasion:

1. intrusion into one's private life and affairs;
2. public disclosure of embarrassing private facts;
3. unwanted publicity of private individuals; and
4. misappropriation of a name or likeness for financial advantage. [52]

"First identifying the harm, a right of privacy is predicated on mental anguish and feelings, that in and of themselves, were an actionable right to protect." [56]

The Warren and Brandeis article proved to be immensely influential. Twelve years after its 1890 publication, *Roberson v. The Rochester Folding Box Company* (filed in 1902 in New York's Court of Appeals) catapulted the case to national attention. A 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 Roberson without her prior knowledge or consent. "In addition, the lower right hand corner, in smaller capital letters, stated, 'Rochester Folding Box Co., Rochester, N.Y.'" Though the majority opinion held that a right to privacy had not yet found its way into jurisprudence, and thus it could bring a civil action against the Rochester Folding Box Company, it cited Warren and Brandeis' article and declared 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." [48] However,

> 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." … 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. [48]

The New York State legislature did not ignore the majority opinion in *Roberson*. A year later, in 1903, it enacted Sections 50 and 51 of the New York's Civil Rights Law. 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. [42]

With this, a right of privacy had been incorporated into state law in the United States for the first time. Other states followed New York.

Not long after this, the Supreme Court of Georgia actually recognized a legal "right to privacy" in *Pavesich v. New England Life Ins. Co.* (filed in 1904, decided in 1905). The court found that using a picture of a plaintiff for an advertising campaign without the plaintiff's consent could be considered libelous and recognized this as a violation of the plaintiff's legal right to privacy [29]. Lawmakers' reactions to the ability for the camera to capture information without giving a subject notice is seen in a bill introduced in Congress in 2009 that wanted to require all film or digital cameras to make a noticeable "shutter sound" while taking a picture, so that any subjects of that picture would have some degree of notice.

The camera's potential to change the integrity of information was not ignored by the law either. In Illinois in 1985, a woman's picture taken for *Playboy* magazine was later printed in *Hustler* magazine [26]. She sued *Hustler* and won, because "*Hustler* insinuated that she was willing to appear nude in a 'degrading setting'", which was not the terms with which she consented to appear in this photo for *Playboy* [25]. The court ruled in her favor, recognizing an injury to her reputation, not because *Hustler* didn't have a right to the picture but because *Hustler* hadn't sought consent from her to appear in the picture *as they presented it.* That *Hustler* was able to alter the context of the picture is an example of photographic printing techniques' ability to compromise the integrity of information.

The camera opened up questions about the extent that American society valued reputation. Legal scholars and the public reacted specifically to the ways it disrupted the six information DOITs of our lens, and we contend that it is in looking at these changes that we understand what the camera showed us about privacy. Warren and Brandeis called for a tort that protected the "public disclosure of private facts"— this resembled the English Breach of Confidence tort. Today, this tort is actively used and at times even used to understand the limits of the right to freedom of speech.[2] The public and legal

---

[2] See *Kinsey v. Macur*, 107 Cal. App. 3d 265, 165 Cal. Rptr. 608 (1980)

reactions to these technological changes—specifically to the changes they made to the DOITs of our lens—indicate that American society valued reputation just as much as English society always had. It sought to protect reputation by protecting the right to be let alone, by enacting a "Right to Privacy". The Right to Privacy was needed to protect one from situations that could lead to a reputation being tarnished—it was a stronger right than the right to accuse someone of slander, libel or defamation, because it delegitimized situations that could lead to one of these, even if an actual libelous act never occurred. By examining the reactions of society to the camera's potential to infringe on privacy, we have discovered that one of the reasons society values privacy is that privacy protects reputation. American society first conceptualized the right to privacy as the right to have one's reputation protected from situations that could tarnish it. It thus saw privacy as a state where one could act as one chose without any consequences on one's public reputation. It felt everyone deserved a right to this state.

7.2 The Telephone and the Fourth Amendment

The invention and widespread adoption of the telephone brought the potential for recording two new types of information: the audio information exchanged in a telephone call and the record of the call's endpoints that a telecommunications provider would maintain. Though neither form of information was new, the telephone caused these forms of information to exist on a scale that spurred changes in privacy law.

7.2.1 Technological Changes

7.2.1.1 Audio Information

Face-to-face conversation, letter writing, physical messengers, and telegraphy were common forms of communication when, in the early 20th century telephones became staples in American households. However, the nature of these prior communication modes meant that information exchanged was hard to intercept: Face-to-face conversation gave participants the agency to control the circumstances in which they exchanged information, which limited the opportunity for interception. As discussed in Section 6.4, eavesdropping was punishable both under England's Common Law and in the United States. But cases citing eavesdropping indictments were rare. Further,

> [Though letters] were vulnerable, intercepting one was still a hit-or-miss affair. Messages traveled by a variety of postal services, couriers, travelers, and merchants. Politically sensitive messages, in particular, could not be counted on to go by predictable channels, so special couriers were sometimes employed… And written messages enjoyed another sort of protection. Regardless of a spy's skill with flaps and seals, there was no guarantee that, if a letter was intercepted, opened, and read, the victim would not notice the intrusion. Since spying typically has to be done covertly in order to succeed, the chance of detection is a substantial deterrent. [24, p. 174]

Letter surveillance was therefore difficult to orchestrate and came with a substantial chance of detection. As the laws discussed in Section 6.6 explain, it was also illegal. Telegraphy is the closest predecessor to telephony. Telegraph wires transmitted written messages long distances, and they could be tapped. But once again there were laws preventing this. The earliest law against tapping telegraph wires was passed in 1862 by California's legislature. This law was used to prosecute a stockbroker in 1864 who tapped wires to gain market information. Other states had similar laws. The laws were usually worded to "forbid the act of wire tapping among other interferences with the telegraph system or specified kinds of property damage to the telegraph company" [44, p. 514]. Furthermore, "Prosecutions under these provisions seem to have been rare." Police officers had used wiretaps with the telegraph but "[they] were not tried for wiretapping because it was thought that the law didn't apply to them" [63, p. 537]. Telegraphy reached its peak in 1870, where 211 million telegraphs were handled internationally. Neither telegraphs nor wiretaps on telegraphs were particularly widespread.

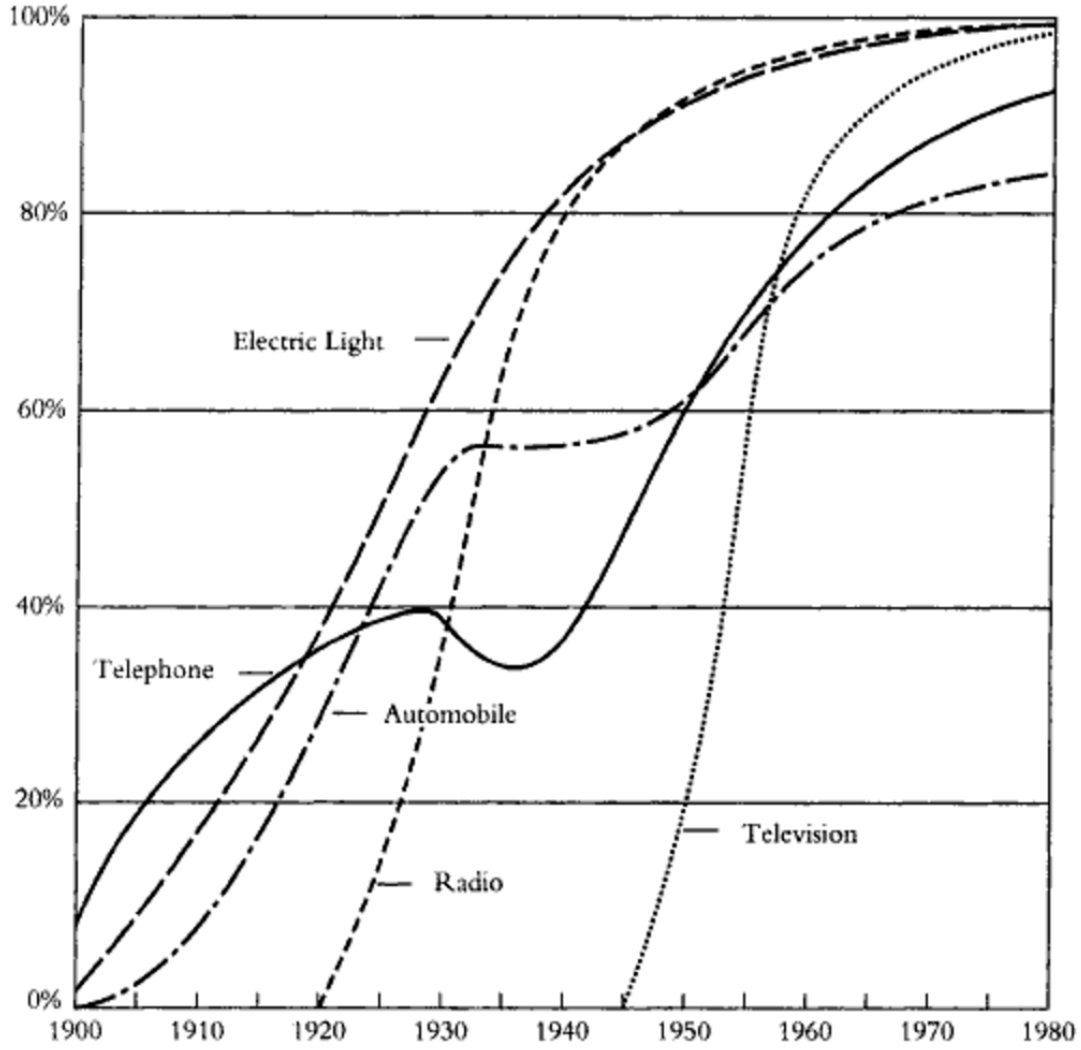
The decline of the telegraph comes with Alexander Graham Bell's 1876 patent of the telephone [51]. In contrast to the telegraph, the telephone grew rapidly as a technology and as a target of wiretapping. In July 1877, shortly after receiving a patent for the telephone, Alexander Graham Bell and two of his backers formed the Bell Telephone Company. They pushed for opening the first telephone switchboard in New Haven in January 1878, allowing any subscriber to this switchboard to be connected to any other. "By mid-1878[,] the telephone business was in ferment. About 10,000 Bell instruments were in use throughout the nation" [30, p. 36]. Bell and its competitors, seeing the quick adoption by consumers of their Telephone services, rushed to claim territory:

> Between February and April 1878, the first exchanges opened in California, New York, Delaware and Massachusetts. The growth was so sudden that the U.S. Census Bureau confessed in 1880 that neither it "nor any statistical agency can deal in a wholly satisfactory manner with anything which is subject to rapid and violent changes." [30, p. 87]

Companies aggressively marketed the telephone, seeing in it a far greater opportunity for profit than they had in the telegraph. John I. Sabin, the President of Pacific Telephone and Telegraph (PT&T) boasted in 1900:

> It is the purpose of the management to extend the use of the telephone to every town, no matter how small, throughout the Pacific States; and in all of the cities and towns, to put a telephone, at most reasonable rates, within easy and immediate reach of every person whose income is sufficient to permit him to ride on street cars. [30, p. 88]

Citizens and businesses alike readily welcomed the telephone. In a 1902 census report, California was found to have the world-leading rate of 111 Telephones per 1000 residents, which the report credited to the "assiduity with which the telephone habit has been cultivated by the managers of companies." [30, p. 88] The same report declared the total "estimated number of messages or talks" on all phone lines in the United States to be 4.9 billion. In 1907, this number was up to 11.2 billion. The telephone's popularity had dwarfed the telegraph's within only a decade of the former's invention. As Figure 1 shows, 40% of all American households had a telephone line by the mid 1920s.



Note: Smoothed lines.

FIGURE 1. U.S. HOUSEHOLDS WITH SELECTED CONSUMER GOODS, 1900–1980. This figure shows how several domestic technologies spread among Americans in the twentieth century. Slowed in part by the Depression, the telephone and automobile did not diffuse as rapidly as the three electronic devices. (Source: U.S. Bureau of the Census, *Historical Statistics* and *Statistical Abstract 1990.*)

Figure 1: Households adopted the Telephone rapidly

American business increasingly began using the telephone—as did bootleggers.

The “lawless twenties,” or the Prohibition Era, was characterized by bootleggers using telephones to conduct smuggling operations [44, p. 514]. Though statistics about this practice are difficult to find, court cases help show that law enforcement was well aware of it—and employed wiretapping to apprehend these smugglers.

In 1928 in Washington State, almost entirely based on evidence from wiretaps, Roy Olmstead was convicted of running a $2 million-a-year bootlegging operation. He appealed this conviction on the grounds that the wiretaps were warrantless, and his case was eventually heard in the Supreme Court. The court invoked a 1914 case, *Weeks vs. United States*, in which evidence obtained by a violation of the Fourth Amendment was found not admissible in court. The burden before the court, then, was to decide whether wiretapping constituted a violation of the Fourth Amendment. If it did then the evidence of his smuggling obtained using wiretapping would be inadmissible, and Olmstead would probably be acquitted; if it didn’t then Olmstead’s conviction would be upheld. The court ruled 5-4 that wiretapping did not constitute a search or seizure of Olmstead’s private property under the Fourth Amendment, because the wiretaps were installed without trespass onto his physical property. Although the law in effect at the time related to wiretapping, Section 27 of the Radio Act of 1927 did explicitly outlaw the “intercept[ion]” and “divulge[nce]” by any person of the “contents, substance, purport, effect, or meaning” of “radio communications” to “any person other than the addressee, his agent, or attorney”, the court decided that “any person” did not construe federal agents [43]. The court also quashed suggestions that this was a breach of Olmstead’s Fourth Amendment rights by declaring, “the words ‘search’ and ‘seizure’ cannot be construed to prohibit gathering of evidence by hearing or sight” [44, p. 528]. This decision implied that eavesdropping could not be considered a violation of the Fourth Amendment, a precedent that was met with chagrin by Justice Louis Brandeis. In a dissenting opinion, he said that the Fourth Amendment should extend to telephone conversations. He didn’t want the term “search” to be interpreted so literally as to only punish physical searches. According to him “They, should be interpreted to prevent the ‘subtler and more far-reaching means of invading privacy’” [44, p. 529]. He also drew attention to the agents’ violation of the Radio Act of 1927.

In the years after this 1928 decision, interstate telephone lines rapidly increased in number. In 1914, the Supreme Court had set a precedent in *Houston, East & West Texas Railway Co. v. United States* that gave the Interstate Commerce Commission the authority to set maximum prices on interstate transport. Lobbyists and President Roosevelt wanted to establish a body to regulate on the telephone and other communications technologies, particularly because of their increasing interstate flavor. So President Roosevelt wrote a memo to Congress advocating for the creation of a regulatory body that will

> be vested with the authority now lying in the Federal Radio Commission and with such authority over communications as now lies with the Interstate Commerce Commission—[it should regulate all] the services which rely on wires, cables, or radio as a medium of transmission. [28]

Following this, the Communications Act of 1934 was passed, establishing the Federal Communications Commission. Section 605 of the Act repealed Section 27 of the Radio Act of 1927 and instead provided:

> Unauthorized publication or use of communications. No person receiving or assisting in receiving, or transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, to any person other than the addressee, his agent, or attorney, or to a person employed or authorized to forward such communication to its 'destination, or to proper accounting or distributing officers of the various communicating centers over which communication may be passed, or to the master of a ship under whom he is serving, or in response to a subpoena issued by a court of competent jurisdiction, or in demand of other lawful authority; and no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person; [3] and no person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by wire or radio and use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto, [4] and no person having received such intercepted communication or having become acquainted with the contents, substance, purport, effect, or meaning of the same or any part thereof, knowing that such information was so obtained, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of the same or any part therecf, or use the same or any information therein contained for his own benefit or for the benefit of

> another not entitled thereto: Provided, That this section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication broadcast, or transmitted by amateurs or others for the use of the general public, or relating to ships in distress [21].

The legislative history of Section 605 is recorded in a Committee report stating that it "is based upon Section 27 of the Radio Act and extends it to wire communications". A chance for the Supreme Court to interpret this legislation came the very same year it was passed in *Nardone v. United States*,

> The defendants, under indictment for smuggling alcohol, objected to testimony of federal agents to the substance of interstate communications overheard by them through tapping of telephone wires. The Supreme Court, reversing the judgment of conviction, held that under the second clause of Section 605, "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect meaning of such intercepted communication to any person", the phrase "no person" comprehends federal agents and that the ban on communication to "any person" bars testimony to the content of an intercepted message. [40]

The court was criticized for this decision by the Government because it felt that, in general, words in a statute are not applicable to the government and that the court's interpretation of this law might facilitate crime[3]. The court felt that,

> Congress may have thought it less important that some offenders should go unwhipped of justice than that officers should resort to methods deemed inconsistent with ethical standards and destructive of personal liberty. The same considerations may well have moved the Congress to adopt Section 605 as evoked the guaranty against practices and procedures violative of privacy, embodied in the Fourth and Fifth Amendments of the Constitution. [40]

Thus, wiretapping and, consequently, the covert capture of audio information without a citizens' consent now constituted a violation of the Fourth Amendment.

This precedent now preempts previous laws related to eavesdropping and extends to any form of electronic spying. The next task for the court was determining which breaches of audio privacy to consider violations of the Fourth Amendment. "In 1961 in a

[3] See 53 Harvard Law Review 863 (1940).

case tried as *Silverman vs. United States*, police pushed a “spike mike” through a party wall of an adjoining house until it touched the heating duct in defendant's house, thus converting the entire heating system into a conductor of sound. Defendants were convicted, and the court of appeals affirmed, based on testimony that the microphone did not penetrate more than five-sixteenths of an inch. In a unanimous decision, the Supreme Court reversed, refusing to base their reasoning on the technicality of trespass, but upon the reality of an actual intrusion into a "constitutionally protected area" under the Fourth Amendment. This new “test” for what could be considered a breach of the Fourth Amendment was further defined in 1962, when it was argued that monitoring a jail cell conversation was a violation under the test. Although the Court rejected the petition, it broadened the area to be protected to include an apartment and hotel room, and in some cases, a store or business office.” In *Charles Katz vs. United States*, the court expanded this definition to a widely used litmus test in determining breaches of privacy today: the “legitimate expectation of privacy” test. Federal agents overheard Katz transmitting gambling information by monitoring a bug that they installed on the outside of a public payphone that he used. He was acquitted because the evidence obtained was considered a breach of the Fourth Amendment, because he had a “legitimate expectation of privacy”. Thus the law “arrived at the current view of bugs and wiretaps as a form of search: that they are permissible but subject to the limitations and protections laid down in the Fourth Amendment” [24, p. 189].

Written records

For billing and other purposes, telephone companies have always kept written records of telephone calls that customers make. Section 220 of the Communications Act of 1934 act demands that carriers keep customers’ records in a certain way. The closest predecessor to this kind of information that sheds some light on how it is understood is the census. In 1840, when the census added questions about employment and family members, some people objected that the census was obtaining information about their “private affairs.” [50, p. 145] In response to this, the Census Bureau responded “Such however, is not the intent, nor can be the effect, of answering ingenuously the interrogatories. On the statistical tables no name is inserted—the figures stand opposite

no man's name; and therefore the objection can not apply. It is, moreover, inculcated upon the assistant that he consider all communications made to him in the performance of this duty, relative to the business of the people, as strictly confidential" [50, p. 145].

In keeping with this assurance of confidentiality of recorded information, Section 220f of the Communications Act of 1934 provides that "No member, officer, or employee of the [FCC] shall divulge any fact or information which may come to his knowledge during the course of examination of books or other accounts, as hereinbefore provided" except if directed to do so by the FCC, a court, or by the customer themselves [47 U.S. Code § 220 - Accounts, records, and memoranda]. Section 222 states "Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of … customers." [47 U.S. Code § 222 - Accounts, records, and memoranda]

At first, people were protected from the Government accessing their phone records without a warrant and from companies disclosing their information to anyone else without their consent. However, this law doesn't extend far: In 1979 in Maryland, a telephone company installed a "pen register" at its central offices to record the numbers dialed from a suspected robber's phone. The suspected robber petitioned the court to strike down evidence found using the pen register as a violation of his Fourth Amendment rights. But the court held that:

> 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." [29]

The court also cited a case in 1977, *United States v. New York Telephone Co.* in which it was decided that installation of pen registers did not need a warrant under Title III of the

Omnibus Crime Control and Safe Streets Act of 1968, the most recent law requiring warrants for wiretaps.

Laws emerged that emulated the standards set by Section 220 of the Communications Act of 1934, requiring customer consent or legal directive before proprietary information could be divulged to anyone else[4]. However the value of this information was not lost on businesses. There began a practice of buying and selling this kind of information—call records and other data that businesses possessed about their customers, so called "data brokerage". By the 1990s in the United States, there were "over 500 commercial databases buying and selling information" about people [24, p. 154]. These data brokers claim they are operating within the law, trading only information that is publically available. The extent of this practice, and its potential harms to individuals, as exposed by Dr. Latanya Sweeney previously, inspired the Electronic Privacy Information Center (EPIC) to petition to the FCC to tighten the laws and standards designed to protect call records maintained by telecommunications providers. In response, the FCC released the report[5] titled "Data Security: Protecting the Privacy of Phone Records" which reiterated that all customer call records maintained by telecommunications providers can only be disclosed to others if the FCC, a court, or the customer to whom the record pertains directs the provider to do so. It hypothesized that hacking the providers' databases and "pretexting" were major causes of data brokers having call records, and it suggested measures to telecommunications providers to better secure their data. It further suggested that providers should make "audit trails that record all instances when a customer's records have been accessed and whether information was disclosed, and to whom;" [29] It categorically declared the illegality of "pretexting", as discussed below.

In 2006, Patricia Dunn the chairwoman of HP's board, hired an independent security agency to investigate her own board following an information leak. "[They] engaged in 'pretexting'—calling up phone companies and impersonating directors

---

[4] See Federal Privacy Act of 1974 protecting personal information in Federal databases, Video Privacy Protection Act of 1988 which prohibits the release of video rental information etc.

[5] Accessible at research.policyarchive.org/2755.pdf

seeking their own records", which the phone companies gave out [37]. The targeted directors sued HP for millions, and Dunn was ousted. Congress looked seriously upon this incident as grounds to pass the Telephone Records and Privacy Protection Act that declared a 10-year prison sentence to anyone found guilty of such "pretexting". The FCC report reiterated this law.

7.2.2 Discussion with respect to lens

Type. Exchange of audio information and records are not new—but the telephone vastly increased the exchange of audio information over easily intercepted channels. It enabled people to convey information they would otherwise have to convey in person, but changed the channel over which this information was conveyed, creating a new type of information. Call records were a new kind of record that revealed people's telephone numbers (which recently have begun carrying area codes); the record of telephone numbers also contained records of the customer's address, sex, etc. which could be used to compare against other records. The extent to which people used the telephone also vastly increased the quantity of this kind of recorded information about people.

Fidelity. Telephone communication didn't suffer from the constraints that telegraph or epistolary communication did—it almost perfectly emulated face-to-face conversation, at least in terms of the audio information that could be exchanged between the interlocutors. Thus, communication over the telephone lent itself to much richer discussion of detail than communication over prior forms of long distance communication.

Notice or Consent. When telephone wires are tapped, no notice is given to the people on either end of the phone call. Unless the participants are aware another person is present to their phone call, it is implied that they have not given consent to that person listening to their exchange of information. The ease and widespread practice of wiretapping telephone wires reduced the standard of notice and consent for this audio information to be captured by third parties. With recorded information, when a record about person A kept by company B is viewed by person C, person A has no idea, yet person C has gleaned personal information about person A. Therefore records, a product

of telephone technology, reduce the standard of notice of exchange of this kind of personal information.

Dissemination and Prevalence. The ability to tap audio information exchanged over a telephone call increases its potential for dissemination. The practice of data brokerage shows that once records are created, they can be copied and disseminated widely. Records continue to exist unless they are deleted under specific circumstances. This increases the prevalence of this kind of information.

7.2.3 Reactions and discussion of meaning of privacy

As English law discussed previously shows, society frowned upon eavesdropping for the same reason it frowned upon breach of confidence—because it gave the eavesdropper information that could defame someone's reputation. This was taken into account in early laws related to mail—these laws show that the founding fathers of American society had a similar interpretation of the harms from eavesdropping. By outlawing the reading of mail, they enacted a law that showed the value they placed on "postal privacy". They had recognized the importance of keeping personal communication private, and they wanted it to extend to all forms of personal communication. The Supreme Court judgment that made interception of first-class mail by the government illegal without a warrant found it constituted an illegal search under the Fourth Amendment. The majority opinion even went as far as to say that this was necessary to protect the "privacy of first-class mail." [58]

American society even went a step further. It made it illegal for government authorities to read private mail correspondence without a warrant. Doing so became a violation of citizens' Fourth Amendment rights—rights against unlawful searches by the government. As discussed earlier, the British colonial authorities would spy on mail as a way of disrupting revolutionary action. That these same revolutionary's, who later became lawmakers, wanted to outlaw the government's ability to spy on its citizens meant they wanted to protect citizens' rights to political dissent. In this action, they showed that privacy protects this right. The Fourth Amendment was put in place because British colonial authorities would invade American citizens' homes and seize their goods

for their own gain, or seeing their goods, impose arbitrary duties on them, again for their own gain. The Fourth Amendment was enacted to protect independence of citizens and limit the government's power. Intercepting citizens' communication was now considered a violation of this amendment, which meant the law allowed citizens to communicate about anything—including their views on the government—without the government able to control such communication. This understanding of the importance of privacy bears resembles Kant and Mill's conceptions of the value of the private realm and independent thinking.

Studying the telephone's influence on our DOITs shows that society still values these conceptions of privacy. As discussed, wiretapping telegraphy was illegal, but the laws were worded more to punish the physical damage of telegraph company property that often resulted from these wiretaps. Prosecutions for wiretapping telegraphs were low in general, and police officers were never tried for this. This changed with the telephone, because it influenced the DOITs in a stronger way than the telegraph could. It created a new form of information with much greater fidelity than the telegraph, which still only delivered written messages. Telephone lines were more widespread and more widely used than telegraph lines, leading to a much greater potential for dissemination of intercepted information. Though both technologies reduced the standard of notice when information was being intercepted, telephone information was intercepted without notice on a much greater scale, simply because there was so much more of it than telegraph information. The whole-heartedness with which American businesses and consumers adopted telephone service gave it a monopoly over communication that the telegraph never had. This also created a situation where those interested in intercepting one's communication knew exactly how to do so—since everybody began using the telephone to communicate.

Thus, though laws existed outlawing wiretapping telegraphs, and the Radio Act of 1927 outlawed wiretapping telephones from very early on, it was because of the telephone that these laws began extending to the government as well. In *Olmstead* and *Nardone*, a situation created as a result of the telephone, allowed legal scholars an opportunity to examine the powers of the government, and uphold privacy as the device with which government powers would be curbed.

Police were never tried for wiretapping telegraphs, but they were tried for wiretapping telephones. When the technology didn't interfere with our DOITs enough, society was content to let certain privacy infringements go unnoticed. Yet, as soon as the technology interfered enough with the DOITs to trigger conversations about privacy and test what society values as private, society might show that is prepared to go to great lengths to protect what it values as private. In *Nardone*, the Fourth Amendment was being interpreted to protect a criminal and incriminate law enforcement—yet because of the immense value of privacy, this interpretation stood.

The telephone reinforced certain longstanding societal values, but challenged others. In *Smith*, the Supreme Court felt that one doesn't have a reasonable expectation of privacy regarding information already divulged to someone else (this so-called "third-party principle" will be discussed in greater detail in the next subsection). With the advent of telephone records, we can understand a little more about how society comes to consider something private. Though laws always protected call records from being disseminated to others, data brokers still managed to access them, and this wasn't given serious attention till the information in call records was used to glean intimate facts about people. Once it was realized that call records contain information that could uniquely identify people and harm reputations, society reacted with stronger laws and information security standards. Further, as evidenced by the FCC's call for telecommunications providers to audit all information trails, when the potential for a piece of information to harm reputation is realized, it causes society to tighten its vigilance over other forms of information that could do the same. The telephone created information that could be put to this use, forcing society to question its understanding of privacy. This is the beginning of a trend that we will see emerging with the next two technologies: as more information about people is publically available, data from various databases can be cross-referenced and individuals can be identified from seemingly "anonymous" data. Data that was innocuous can now become a key to uniquely identifying someone. Once someone is uniquely identified, a stranger could potentially learn intimate details and affect a reputation. As we have seen from previous analysis, humans put great stock on their reputations, so giving someone control over an individual's reputation gives a lot of

control over that individual. This idea of privacy protecting independence—protecting individuals from being controlled—will be discussed further below.

This idea ties to a discussion of another conversation the telephone started: the extent to which the government has bent carefully established privacy laws for the purpose of law enforcement and intelligence. Even though wiretapping is illegal without a warrant, it can be undertaken with a warrant. Still, today, phone records can be obtained from telephone companies by subpoena. In 1954, President Eisenhower's attorney general Boswell petitioned Congress to allow warrantless wiretaps to spy on and prosecute Communists. Although the proposal was denied, FBI director (and founder) J. Edgar Hoover wiretapped suspected Communists extensively, anyway. He is thought to have possibly wiretapped Congressmen and known to have wiretapped Supreme Court justices [24, p. 185]. In 1994, President Clinton signed into law the Communications Assistance for Law Enforcement Act (CALEA) "to enhance the ability of law enforcement agencies to conduct lawful interception of communication by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in capabilities for targeted surveillance, allowing federal agencies to selectively wiretap any telephone traffic" [22]. Though regular law-abiding citizens' privacy is protected, as soon as a court decides that someone is a threat to society, a warrant to obtain a lot of information about them would readily be provided. This information gives the government, in some circumstances, an ability to control certain individuals.

That the FCC could only respond to EPIC's petition (discussed above) by recommending that companies improve security standards starts another shift in privacy from ancient times: though individual's may value privacy because of how they values reputation and independence, individuals may not always be able to ensure privacy for themselves—if they need to use a particular service, they have no choice but to comply with the policies of the company rendering them that service's policies. If these policies include record collection and if these records are compromised, then there is nothing the individual can do to prevent a loss of privacy. Studying the telephone's creation of records as a new form of information provides an insight into this trend.

8 Locational Information and the Global Positioning System

8.1.1 Technological Changes

8.1.1.1 Following and Beepers

In 1990, Section 646.9 of the California Penal Code made it illegal to

> willfully, maliciously, and repeatedly follow or willfully and maliciously harass another person and make a credible threat with the intent to place that person in reasonable fear for his or her safety. [15]

It defined a credible threat as

> a verbal or written threat or a threat implied by a pattern of conduct or a combination of verbal or written statements and conduct made with the intent to place the person that is the target of the threat in reasonable fear for his or her safety or the safety of his or her family and made with the apparent ability to carry out the threat so as to cause the person who is the target of the threat to reasonably fear for his or her safety or the safety of his or her family. It is not necessary to prove that the defendant had the intent to actually carry out the threat. [15]

Prior to enactment of this law, if a private citizen in California (or in any other state) felt uncomfortable being followed by another private citizen then a Temporary Restraining Order (TRO) could be requested from the court against this person. “In order to obtain a TRO, the victim must first demonstrate that the harassment [following is considered a form of harassment] would cause a reasonable person to suffer substantial emotional distress” [33]. Under the old law, one couldn’t prevent another person following without proving that the perpetrator’s behavior would cause emotional distress. Under the new law, a credible threat had to be proven. Under either law, no authority could prevent someone following or tracking movements through public places.

The Fourth Amendment, enacted to protect private citizens from the government’s unlawful intrusion into their affairs does not protect information exposed to the public. In 1974, the Supreme Court held that scraping paint from a car that was moved by police from a public commercial parking lot to an impoundment lot was not considered a search under the Fourth Amendment. The Supreme Court reasoned that moving the car to search it was not a violation, because the police had probable cause to suspect the car was used in connection with a crime, but also, notably that the car was

"seized from a public place, where access was not meaningfully restricted" [18]. Justice J. Powell concurring with the judgment, added that

> One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects. A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view. [18].

Nowhere in the scope of United States laws that existed in the late 20th century was following someone through public places in an of itself deemed illegal. In addition, recording someone in a public place by means of photography, thereby creating a record of that person having been in that location was also permissible in the eyes of the law. A report published by the National District Attorney's Association in 2009 shows that in all 50 states photographing someone is considered "voyeurism" (and thereby illegal) only if they do not have a reasonable expectation of privacy [61].

With these laws in place, and even before the stalking law in its current form came to be, several cases emerged in the 1970s and 1980s in which law enforcement was tracking suspect locations and encountered evidence that would be useful to indict them for crimes. The courtroom response and discussion surrounding these cases serves as an effective indicator of the legal understanding of locational privacy at this time. In *United States vs. Moore* (1977), *United States vs. Claybourne* (1978) and *United States vs. Knotts* (1983), law enforcement agents installed radio transmitters known as "beepers" on some part of the suspect or inside a container that the suspect was carrying [29]. All of the defendants in these cases were suspected by law enforcement of producing controlled substances. In *Knotts*, the Minnesota law enforcement officers arranged with a seller to place a beeper into a chloroform container that was sold to the defendant and two accomplices. Monitoring the location of the beeper allowed law enforcement to keep a constant visual surveillance of the defendant and his accomplices and follow them to a cabin in Wisconsin. The officers subsequently obtained a warrant to search the cabin and found markers of the defendant's intent to synthesize amphetamine, a controlled substance. The defendant's motion to suppress evidence based on the warrantless monitoring of the beeper was denied by a Federal District Court. Though the Court of Appeals reversed this on the grounds that such monitoring was a violation of the Fourth

Amendment, the Supreme Court sided with the District Court and found no violation of the Fourth Amendment. Justice Rehnquist, delivering the opinion of the court, declared:

> The beeper surveillance amounted principally to following an automobile on public streets and highways. A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements. While respondent had the traditional expectation of privacy within a dwelling place insofar as his cabin was concerned, such expectation of privacy would not have extended to the visual observation from public places of the automobile arriving on his premises after leaving a public highway, or to movements of objects such as the chloroform container outside the cabin. The fact that the officers relied not only on visual surveillance, but also on the use of the beeper, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting their sensory faculties with such enhancement as science and technology afforded them in this case. There is no indication that the beeper was used in any way to reveal information as to the movement of the chloroform container within cabin, or in any way that would not have been visible to the naked eye from outside the cabin [29].

Undeniably, the court believed that this use of location tracking technology would only be considered a violation of the Fourth Amendment if it afforded law enforcement capabilities that their natural faculties of vision (or other senses) did not afford. If tracking simply enhanced these faculties, but only in a capacity that would not be considered a search without the use of technology, the search would be permissible. Similar judgments were returned in the other two cases. So the view of the law around these earliest uses of technology for locational monitoring was that to be considered illegal, the technology must provide law enforcement with faculties that they didn't naturally possess. If a private citizen or a law enforcement agent could come across a piece of information using their natural faculties on their own, or aided by technology, they could use this information as if it had been given to them with the consent of the person to whom it pertained, and controlling this information flow would not be considered a violation of that person's privacy.

This wasn't the mainstream legal opinion for long. The first inkling of dispute came in *United States vs. Karo* (1984). In this case, DEA agents installed beepers in cans of ether that were sold to the defendant Karo and three other suspects. They installed these beepers with the consent of the seller. They believed that the defendant and others were going to use the ether to extract cocaine from clothes that had been imported into

the United States. Karo moved to have the evidence from these beepers suppressed. The court considered two aspects of the case that might have lent validity to Karo's motion: first that the cans had been sold to Karo without his knowledge of the beepers inside them, second that the DEA had continued monitoring the beepers once the cans were within Karo's private residence, where he had a reasonable expectation that his location and movements would be private. The court stated:

> The mere transfer to Karo of a can containing an unmonitored beeper infringed no privacy interest. It conveyed no information that Karo wished to keep private, for it conveyed no information at all. To be sure, it created a potential for an invasion of privacy, but we have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment… We conclude that no Fourth Amendment interest of Karo or of any other respondent was infringed by the installation of the beeper. Rather, any impairment of their privacy interests that may have occurred was occasioned by the monitoring of the beeper…. private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable. Our cases have not deviated from this basic Fourth Amendment principle. Searches and seizures inside a home without a warrant are presumptively unreasonable absent exigent circumstances… In this case, had a DEA agent thought it useful to enter the Taos residence to verify that the ether was actually in the house, and had he done so surreptitiously and without a warrant, there is little doubt that he would have engaged in an unreasonable search within the meaning of the Fourth Amendment. For purposes of the Amendment, the result is the same where, without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house. The beeper tells the agent that a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched. Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations but also establishes that the article remains on the premises. Here, for example, the beeper was monitored for a significant period after the arrival of the ether in Taos and before the application for a warrant to search. [29]

The court thereby reversed the judgment of the Court of Appeals that had found against a Fourth Amendment violation. In the above judgment, the Supreme Court made it clear that had one of the DEA agents entered the Taos residence without a warrant to make sure that the ether was actually in the house "there is little doubt he would have engaged

in an unreasonable search within the meaning of the Fourth Amendment." However, in another case involving narcotics, the court declared a similar search lawful: In *Ker v. California* (U.S. 1963), officers from the Los Angeles County Sheriff's department followed George Ker after seeing him meet with another suspected drug-dealer they had been tracking. Though they lost him, they had noted down his license plate number and traveled to an address obtained from that license number from the Department of Motor Vehicles. After ascertaining that there was someone in Ker's apartment, they obtained a passkey from the building manager to enter his apartment without a warrant. When they entered, they introduced themselves as narcotics officers and saw George Ker's wife Diane emerge from the kitchen. One of officers walked towards the kitchen and without entering it, observed through an open doorway "a small scale atop the kitchen sink, upon which lay a 'brick-like—brick-shaped package containing the green leafy substance' which he recognized as marijuana." [29]. The Supreme Court found no violation of the Fourth Amendment in entering the apartment without a warrant to arrest George Ker, because of the overwhelming probable cause that the officers had. However, in upholding the probable cause to arrest Diane Ker, the court had this to say:

> Probable cause for the arrest of petitioner Diane Ker, while not present at the time the officers entered the apartment to arrest her husband, was nevertheless present at the time of her arrest. Upon their entry and announcement of their identity, the officers were met not only by George Ker but also by Diane Ker, who was emerging from the kitchen. Officer Berman immediately walked to the doorway from which she emerged and, without entering, observed the brick-shaped package of marijuana in plain view. [29]

Clearly, the court didn't find the same violation of locational privacy within private dwellings by a human law enforcement agent (in this case Officer Berman) traveling from one room to another as it did in the Karo case of monitoring the movements of the ether cans within private dwellings. As stated in the court's own opinion in *Karo*, such movements would be easily viewable by the naked eye of an officer who was inside the private Taos residence, as was exactly the case with Officer Berman seeing the brick of marijuana in *Ker*. However, in *Karo*, because this information was supplied by technology, it was considered a privacy violation. In *Ker*, the same discovery, not made by technology was not considered a privacy violation. In this inconsistency, the role of technology in informing privacy is clear. Thus Justice Rhenquist's words in the *Karo*

opinion are not wholly sound: It is not the case that "nothing in the Fourth Amendment prohibited the police from augmenting their sensory faculties with such enhancement as science and technology afforded them". The juxtaposition of these two cases shows that, in the eyes of the law, there are cases when technology enhances what is otherwise naturally possible a little too much, and thereby results in illegal breaches of privacy.

The court itself admitted this in *Kyllo v. United States* (U.S. 2001), where agents used a thermal imager to scan for heat lamps the home of the defendant who was suspected of growing marijuana. Thermal imaging coupled with information from utility bills showed likely use of these heat lamps. On these grounds, agents obtained a warrant to search Kyllo's home where they found more than 100 plants of marijuana. They arrested him for growing marijuana. The Supreme Court found the evidence from the imaging to be inadmissible because thermal imaging was not seen as a legal search under the Fourth Amendment. Voicing the court's opinion, Justice Scalia said:

> We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search. [29]

8.1.1.2 GPS

Parallel to these cases, researchers were fervently racing to invent the best navigation system for the United States' military. In 1958, William Guier and George Wiffenbach at Johns Hopkins' Applied Physics Laboratory attempted to pinpoint a user's location given a satellite's location—the previous year these two physicists had realized they could pinpoint the Soviet Union's man-made satellite, Sputnik 1's location, by observing the Doppler effect on its radio transmissions. This led, in 1960, to the successful test of the TRANSIT system by the United States Navy. These technologies were not used commercially, so do not enter into our discussion of privacy.

However, TRANSIT was too slow for high-speed Air Force operations, and in 1973 the Global Positioning System project started. It originally used 24 satellites. It was initially for military use only. However

> In 1983, Soviet jet interceptors shot down a Korean Air civilian airliner carrying 269 passengers that had mistakenly entered Soviet airspace.
>
> Because crew access to better navigational tools might have prevented the disaster, President Ronald Reagan issued a directive guaranteeing that GPS signals would be available at no charge to the world when the system became operational. The commercial market has grown steadily ever since. [57]

Following this directive, civilian use of the GPS has skyrocketed[6], as has its use by law enforcement[7]. A chance for the Supreme Court to opine on the relationship between GPS surveillance and the Fourth Amendment came in *United States v. Jones*:

> [Agents had a warrant to install a GPS surveillance device on a suspected drug dealer's car]. The warrant authorized installation in the District of Columbia and within 10 days, but agents installed the device on the 11th day and in Maryland. The Government then tracked the vehicle's movements for 28 days. It subsequently secured an indictment of Jones and others on drug trafficking conspiracy charges. The District Court suppressed the GPS data obtained while the vehicle was parked at Jones's residence, but held the remaining data admissible because Jones had no reasonable expectation of privacy when the vehicle was on public streets. Jones was convicted. The D. C. Circuit reversed, concluding that admission of the evidence obtained by warrantless use of the GPS device violated the Fourth Amendment.

The Supreme Court upheld the D.C. Circuit court's reversal. Although, for Justice Scalia, voicing the opinion of the court, the monitoring was not what was considered a violation of the Fourth Amendment, because the location information monitored was on public roads; it was the physical intrusion on the defendant's property, in installing the device, that was an impermissible search. This was not a reaction to the potential privacy implications of locational information. However, Justice Sotomayor's concurring opinion was. She considered the richness of information available from GPS surveillance constituted a search, and she even disagreed with the suggestion that there is no reasonable expectation of privacy because much of this information had been disclosed to third parties. In her concurring opinion she says:

---

[6] Tens of millions of civilians were using GPS in 2008, through car mounted and mobile devices according to market analysis firm Canalys. (https://www.canalys.com/newsroom/gps-smart-phone-shipments-overtake-pnds-emea)

[7] See "Evidence of Use, Suggestions of Abuse" in Yale Law Journal Online
See "Law Enforcement's Uses of GPS Technology" in https://fas.org/sgp/crs/misc/R41663.pdf

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks ... I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

According to her, constant information gathering was an entirely new privacy threat. The government should not be able to benefit from constant information gathering since they didn't have such information when the Fourth Amendment was written, and since this level of information gives power that the spirit of the Fourth Amendment blocks.

In 2013, an article in *The Atlantic* contextualized the discussion of the "third-party principle"—the idea that you do not have a reasonable expectation of privacy regarding information already relinquished to a third party. The government in *Jones* advocated this point, asserting that since people relinquish location information to websites and applications when they carry their phones around, this information should not come with an expectation of privacy from the government. They argued:

> In its 1979 decision in *Smith v. Maryland*, the Supreme Court ruled in favor of the government, observing that "this Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties…
>
> Nojeim argued that "If strict application of the doctrine ever served us well, it no longer does, leading to absurd results. This is particularly true in an age where so much more information is communicated through intermediaries." Kerr countered by stating that "I think that the much-maligned third-party [principle] is a critical tool for applying the Fourth Amendment to new technologies in some cases, but that it should not be extended to all cases ... Importantly, my defense of the third-party [principle] implies an important limit: The doctrine should apply when the third party is a recipient of information, but it should not apply when the third party is merely a conduit for information intended for someone else." … However, in United States v. Maynard, 4 the D.C. Circuit held that warrants are required for law enforcement use of GPS tracking devices. In distinguishing Knotts, the D.C. Circuit pointed to the vast differences between the relatively primitive beeper technology used almost thirty years ago and the unprecedented power of GPS surveillance… Unfortunately, in drawing lines between technology such as powerful binoculars that merely enhance the senses of law enforcement officials and technology such as thermal imaging devices that create new superhuman powers, the Justices have offered confusing guidance to lower courts. At times, they have relied on a distinction between sense enhancement and sense

> creation, a superficial distinction that fails to delineate when new surveillance technology is problematic.

The court ultimately disagreed, but the debate about the third-party principle remains relevant and current, particularly because of data that telephone companies and apps using location-based services collect. In fact, the California Online Privacy Protection Act gives that state's citizens agency to protect themselves from the third-party principle. This law prohibits transfer of a customer's information without consent and gives an individual a right to remove any information any company has collected about that individual.

The FCC's guidelines for companies collecting location-based information is consistent with this law. It recommends that companies give consumers the right to remove any information pertaining to them that the companies have collected. AT&T and PositionLogic, a company that makes location-tracking devices for law enforcement, assert in their privacy policies compliance with the FCC's standards. However, they both explicitly state that in matters of law enforcement they will comply with government requests. Apple and Google say that they notify consumers who use their location-tracking services that these individuals are relinquishing the privacy of their location from the government due to the third-party principle. Their assumption is that if a customer opts in after being informed about this relinquishment of their privacy, the customer has consented to lose control of the flow of their locational information. [60].

In 2015, *The Week* published an article declaring that "privacy advocates are raising objections over police placement of tiny GPS trackers in commonly stolen items" [5]. In the same year, Long Island police were investigating a spree of robberies. They planted a GPS device inside a stack of bills located in a store that they believed the suspect would rob from. A robbery did occur. Within days they tracked a suspect down and arrested him for these robberies, using information from the GPS tracker. The Jones ruling didn't cover cases in which suspects stole items that unbeknownst to them, could be tracked by GPS technology. This is an open area of law, but similar to *Roberson* in the camera section, privacy scholars see the potential of such information to be put to a

different use than its collection was initially authorized. This relates to the integrity DOIT.

> "As a baseline, I don't think people should be tracked with GPS without a warrant," said Jay Stanley, a policy analyst with the American Civil Liberties Union. "If somebody steals an object and the police don't arrest them for six months and just collect information about how they're living their life, that could be problematic." [64]

Many uses of GPS by law enforcement are still under discussion in courts and legal bodies, indicating the extent to which privacy implications of GPS technology are still being evaluated.

8.1.2 Discussion with respect to lens

Type. Knowledge of someone's whereabouts is not new, but geographical coordinates and the ability to trace a path of their locations over some period of time is. Beeper's achieved this partially, estimating coordinates by mapping the beeper's distance from various receivers, but the GPS gives rich, accurate coordinates, anywhere on the planet.

Fidelity. The GPS has satellites whose sole job is pinpointing exact coordinates, accurate within inches of any GPS device. Moreover, GPS devices are able to store and divulge the history of a target for many months, some even for years. This exceeds the capability of the human eye or other prior location tracking technology. As location-tracking technologies became more sophisticated, the law began changing to curb use.

Dissemination. Consumers using location-based services on smartphones can broadcast their location. GPS devices used in law enforcement can be remotely monitored. This degree of accessibility to locational information made available by GPS technology surpasses any of its precursors.

Notice or Consent. GPS devices can be as small as fingernails, light, and silent. As the GPS devices embedded in wads of notes in the Long Island robbery case shows, they can be planted on a person's body and used to track that person's location without notice or consent. It is for this reason that Apple, Google and other makers of location-based

technologies require users of these technologies to provide consent to the tracking of their location.

Prevalence. GPS devices installed legally to track someone's location over an interval of time do not necessarily cease functioning after this period. They can keep tracking someone long after a warrant has expired. Furthermore, access to someone's GPS enabled smartphone or other GPS device gives access to their locational history. This information could potentially be very personal.

8.1.3 Reactions and discussion of meaning of privacy

Before the advent of location-tracking technology in any form, following someone on a public road was not considered illegal. Similarly, photographing people in places where they didn't have a reasonable expectation of privacy was not considered illegal. In these situations there exists a potential to record someone's movements. This is locational information that could be considered personal. However, unless someone had a reasonable expectation of privacy (which doesn't exist on public roads, city streets, state highways, national parks etc.) or someone could prove intent to harm, collection of this information by a third party was not illegal. The potential to record this personal information existed long before location-based technologies, yet the collection of this information was never outlawed.

Though there was some discussion that this precedent should be changed after the government began installing beepers inside the possessions of people suspected of producing controlled substances, it ultimately wasn't changed. As stated in *Knotts*, "Nothing in the Fourth Amendment prohibited the police from augmenting their sensory faculties with such enhancement as science and technology [afford]". The earliest use of location-tracking technology then, still didn't cause society to feel that following someone on a public road was a violation of privacy.

This view dramatically changed as technology became more sophisticated, generated an increasing volume of accurate locational information, and was used more frequently by law enforcement. Records about locational information that technology enabled increased. And as the fidelity of this information afforded by newer technologies

increased, the law was revised. The discrepancy between the ruling in *Karo,* where installation of the location tracker was considered a search (because it created information that an agent without technology could only obtain by trespassing on private property), and *Ker* where an actual trespass wasn't considered a search, is very telling. It shows the court's consideration of privacy implications of technology. Something about the fidelity of information provided by location-tracking technology, and the way it conveys information about subjects to the police without notice lead the court to feel that a person didn't have control over their locational information if location-tracking technology was divulging it. In this case, the court gave people a right to the privacy of this information. When the same information was captured by a human, obtaining this information was not considered a breach of privacy.

As GPS technology began being employed by law enforcement, privacy scholars began noticing more situations where location-tracking took over control of a person's information. In an article for the *Yale Law Journal Online*, Smith et al delineated certain uses of GPS tracking technology by law enforcement, proceeding to establish why these uses were indicative of potential harms to privacy. They write:

> As Daniel Solove notes, outright abuse is not the only threat posed by government information gathering: "even if government entities are not attempting to engage in social control, their activities can have collateral effects that harm democracy and self- determination."

The report thus suggests, at a fairly early stage of GPS use in society (the report was penned sixteen years after the GPS first was first introduced for civilian use) a *potential* for abuse of the Fourth Amendment that GPS technology poses. It criticizes the Supreme Court for placing too much emphasis on the difference between "sense creation" and "sense enhancement" and on the physical intrusions in cases of locational surveillance. It argues that these lenses provide the false impression that consistent monitoring of someone's location, be it on public roads or not would not be a violation of the Fourth Amendment. It purports that this monitoring would very much be a violation of the spirit of the Fourth Amendment—to curb police/government power—were taken into account. Constant surveillance that the GPS enables does offer the police greater power than they could amass over the populace before GPS existed. Thus, law enforcers should have to obtain a warrant before surveilling someone constantly using this technology. They

continue, "[in] cases from Katz to Knotts to Kyllo, wherever a new technology carries the potential for police abuse, the [Supreme] Court has allowed its use only as guarded by the warrant requirement, placing a check on the unlimited discretion otherwise afforded officers". This standard should continue in the case of the GPS, and it should be noted that "there is a vast technical valley between old technologies used by police officers, which merely assist in tailing suspects, and modern GPS surveillance technology, which automates tracking and surveillance."

They feel that GPS is more sophisticated and shows more fine-grained information than the beeper devices of *Knotts* and *Karo*. Where "beepers could neither determine the location themselves nor store that data", the GPS "autonomously calculates latitude, longitude, altitude, direction, and speed by receiving and processing location information from the transmissions of at least four GPS satellites in nearby orbit" and some GPS tracking devices can even store the information internally. "Officers can then manually retrieve the data, or they can do so remotely."

The report goes on to argue that GPS fundamentally alters the reasonable expectation of privacy standard that has been carried through so many cases involving technology and privacy. If GPS surveillance were to continue, one wouldn't have a reasonable expectation of privacy on public roads, as the beeper cases established, but one does have a fundamental expectation of not being surveilled constantly. If surveillance were to be treated as a given, one couldn't claim that one had a reasonable expectation of privacy against the use of this information, but one should definitely have that right, as this is the right the Fourth Amendment was enacted to protect. "Our E-ZPass account records and airline reservations might reveal our comings and goings in broad brushstrokes, but GPS surveillance allows the government to see our micro-level movements: what house of worship we attend, and how often; whether we see a psychiatrist; with whom we spend the night; where we eat; where we exercise; and whether we attend a particular political organization's meetings"

This report calls into question Justice Rhenquist's statements in *Knotts* that suggest that the law would not find a Fourth Amendment violation in any practice that is a mere enhancement of what one can observe naturally, using one's senses in public. The information generated by GPS, though of the same nature as that which can be generated

by the naked eye, has a volume and fidelity the naked eye could never hope to emulate. It is for this reason that the privacy laws related to GPS remain in flux.

Where the discussion around beeper technologies allowed the court to declare that the use of technology to glean locational information about private locations, is unequivocally illegal, it still maintained that gleaning locational information about people on public roads, whether by human visual surveillance or by technological tracking, is legal. However, with the advent of GPS and the question of the third-party principle, privacy advocates are calling this view into question. While nobody is arguing that human following on public roads should be outlawed, privacy advocates, including Justice Sotomayor and the writer's of the *Yale Law Journal Online* article, feel that GPS surveillance provides such accurate information that even tracking someone with a GPS on public roads only should be allowed with a warrant. They feel that GPS provides a greater wealth of information than would be observable by any number of human observers. For this reason, Justice Sotomayor publically argues against the third-party principle. Her opinion generalizes to cases such like online browsing, which is tracked by Internet service providers and companies. She feels that just because they have this information, doesn't mean that consumers don't have a right to control whether the government or anyone else sees it. The California Online Privacy Protection Act, FCC guidelines, and opt-in nature of many location-based services also indicate that society has come to appreciate the privacy implications of GPS tracking, and society wants consumers to have the right to control their locational information whether on public or private property. As the law currently stands, the third-party principle can be applied to locational information, and therefore law enforcement doesn't need a warrant to ask companies to provide locational information about suspects in an investigation. What will happen with this law as GPS becomes ubiquitous remains to be seen.

So information about travels through public property was not considered personal information until the GPS brought the ability to track this travel constantly and accurately, and to record it for posterity. As law enforcement increasingly began to use GPS for these purposes, privacy scholars began considering this information private. The law still operates by the reasonable expectation of privacy standard, but the "private realm", the physical and virtual areas where someone enjoys such a reasonable

expectation of privacy, are shrinking. The size of Mill's "private sphere" is constantly decreasing, giving people a smaller sphere in which they can form independent opinions.

The GPS reprises the conversation that the telephone prompted about individuals' decreasing ability to ensure privacy for themselves. Though the FCC recommends that companies delete personal information on request, the FCC cannot control whether a company actually does this. Though many of these companies require consumers to "opt-in", thereby consenting to their location being tracked, there is no way a consumer can avail of many of these services without consenting to being tracked, whether they really want to consent to this or not. Once location is known by the company, the third-party principle ensures that the government can easily access it. As the privacy policies of most companies state, they will comply with the government and hand over information in matters of law enforcement.

9 Applications of our Lens

Our lens is comprises DOITs, which pinpoint aspects of a new technology that might harm privacy norms, and privacy canaries which help us understand what has always been valued as private in society. This section discusses two applications of this lens. First, we briefly discuss the application to some phenomena enabled by the Internet. Then, we situate our work as a response to prior work in conceptualizing privacy by scholars Daniel Solove and Ryan Calo.

9.1 Privacy Implications of the Internet

9.1.1 Type

The Internet was designed to support a vast array of applications, unlike the telephone or camera, which were dedicated to a particular function. Through the World Wide Web, companies provide an array of services to consumers and create records of the usage of these services. Cheap storage and sophisticated data processing technologies increase what this information can reveal about a person. UK online gaming website FeatureSpace allows users to gamble online. It collects data on the "betting patterns of every one of its customers, including the time of day, frequency and size of bets placed and the types of games an individual typically plays." [Burn-Murdoch] It has begun using this information to, using machine learning, detect gamers that might have a gambling problem. It can use this information as it sees fit, since this information came from tracking user activity, which a user consented to. Yet this information can tarnish someone's reputation, which our privacy canaries showed, is an important value in society.

9.1.2 Fidelity

Tim Burners-Lee, the father of the World Wide Web envisioned it as a decentralized system with no central governing authority. He wanted all programmers to be able to contribute to it with equal access, and give users of it the ability to publish and edit content on it as they saw fit. This offers people power to publish and edit content about others, and when many people corroborate this information, it has a high degree of fidelity in uniquely identifying people or people's attributes. For example, even if you are not "friends" with someone on most social networking sites, you can see who their

friends are. The actions of these people, in publically "befriending" an individual, inadvertently reveal accurate information about the social circle of this individual.

With the Internet, fidelity also works the other way around. Information on the Internet is easily "spoofable" (like setting up a social media profile pretending to be someone else). Further, the standard for information to be considered identifiable on the Internet is relatively low. So a fake social media profile might be accepted as real by people who view it, and it might succeed in tarnishing the reputation of the person it is spoofing. So the Internet facilitates the creation of information with low fidelity that is treated as information with high fidelity. This phenomena on the Internet poses a threat to privacy.

9.1.3 Dissemination and Notice or Consent

Breach of Confidence is a privacy canary in our lens. It states that if a person shares a piece of personal information in confidence with a third party, and if that third party divulges this information, they are guilty of infringing on the first person's right to privacy. The Internet creates situations where one may mistakenly assume a greater degree of privacy about a channel than the channel really provides. For example, a person might divulge certain facts to a select group of friends on a social networking website and one of their friends might comment upon these facts. But the settings of the social network could now make the original set of facts visible to friends of the friend, who are not friends with the original person. This person's confidence has been breached without that person's notice or consent. Another example of dissemination or consent related privacy disruptions over the Internet is the case of technologist Andy Baio's identification of an apparently anonymous blogger. Bloggers frequently use Google Analytics to track page views, a good metric for the success of their blog. Google Analytics IDs of many blogs are publically available. Andy Baio looked up the Google Analytics ID of a particular anonymous blog, and saw that it was the same a blog that provided the blogger's name. He thus correctly concluded that the anonymous blog was run by the person named in the other blog. Unbeknownst to this person, his Google Analytics ID was disseminated openly. This situation lead to a ack of control of his personal identity [9].

9.1.4 Integrity

In 2015 using select segments from publically available videos, a campaign to malign Cornell University's assistant dean of students made it appear that he approved of terrorist training camps on campus. Open access to these videos and freely available online editing tools helped the campaign manufacture a false videotaped interview with the assistant dean. [17] Such information tampering can damage reputation.

9.1.5 Prevalence

All manner of activity on the Internet is recorded and stays accessible. In 2012, the government of India arrested a 21-year old woman over negative comments on Facebook about a politician. They also arrested her friend who had "liked" these comments. [39] Information about people's opinions are widely available to governments or private governing bodies, which can then learn people's opinions and curb potential dissenting behavior. As our privacy canary about Mill's "private sphere" shows, this is an infringement on independent thought.

These are but a few examples of privacy implications of the Internet, but they show how using our lens can structure conversations about how to understand what aspects of the Internet need to be monitored or regulated in order to enact laws that protect the privacy of Internet users. A more in depth conversation about the privacy implications of the Internet that our lens explicates, would be a natural next step to the work we have begun in this thesis.

9.2 Response to Solove and Calo

Ryan Calo, a privacy scholar, has written extensively about technology and privacy. He approaches the discussion of technology and privacy with the same trepidation laid out in the introduction of this thesis,

> … what do privacy violations look like today? They tend to be hard to visualize. Maybe somewhere, in some distant server farm, the government correlates two pieces of disparate information. Maybe one online advertiser you have never heard of merges with another to share email lists. Perhaps a shopper's purchase of an organic product increases the likelihood she is a

> Democrat just enough to cause her identity to be sold to a campaign. At most one can picture the occasional harmful outcome; its mechanism remains obscure… It is hard to know exactly what role the inscrutability of privacy has played in the development of contemporary privacy law. [16]

Calo posits that privacy is "inscrutable" and thus it is hard to put one's finger on what harms contemporary privacy laws are attempting to protect citizens against. He goes on to argue that since "the development of American privacy law has been slow and uneven, but the "advancement of information technology has not", one could map privacy as a series of reactions to "privacy catalysts". His argument suggests that to answer the question "what is it about privacy that causes the Internet to affect it", one must investigate responses from privacy advocates to the Internet, and categorize their responses, their conception of the privacy harms caused by the Internet, as the definition of privacy with respect to the Internet. According to this argument, laws attempting to protect people's privacy from intrusions that the Internet enables should protect people from these specific harms, rather than attempting to reach a definition of the "inscrutable" notion of privacy.

Solove has directly tackled the question of defining privacy in order to understand its relationship with technology and other things. He contends that traditional definitions of privacy tend to label it as one of six things: "(1) the right to be let alone; (2) limited access to the self; (3) secrecy; (4) control of personal information; (5) personhood; and (6) intimacy." [47] He finds each of these definitions too narrow or too broad. He offers situations for each, where because of the narrow or broad definition of privacy, something that would otherwise be considered harmful, to a person is not considered harmful since it is not a specific violation of this specific definition of privacy. For example,

> In *Nader v. General Motors Corp.*, Ralph Nader, a prominent public figure and outspoken critic for consumer safety, criticized the safety of General Motors' automobiles for many years. General Motors interviewed Nader's friends and acquaintances to learn the private details of his life, made threatening and harassing phone calls, wiretapped his telephone and eavesdropped into his conversations, hired prostitutes to entrap him into an illicit relationship, and kept him under pervasive surveillance while outside in public places… The court proceeded to analyze one-by-one each of the particular acts of General Motors. The court held that interviewing Nader's friends

> was not an invasion of privacy… The harassing phone calls and the prostitutes did not involve "intrusion for the purpose of gathering information of a private and confidential nature"… The wiretapping, however, was a well-established tortious intrusion… On the question of the pervasive surveillance, the court held that although observation "in a public place does not amount to an invasion of... privacy," in certain instances, "surveillance may be so 'overzealous' as to render it actionable." … [Solove contends that in this case,] the majority lost sight of the forest for the trees. The purpose of General Motors' plan was to employ its considerable power in a campaign to disrupt Nader's personal affairs. The court should have focused on the way in which the company's actions aimed to disrupt Nader's life, and the paramount social importance of avoiding such exercises of power designed to deter, harass, and discredit individuals… Instead of dissecting the situation and placing each invasion into preexisting categories of privacy, the court should have assessed the whole situation. By slicing off parts of the case and compartmentalizing them into categories, the court impeded a jury's ability to consider the full situation… In short, rather than look for isolated privacy harms based on existing categories, the court should have focused on social practices and their disruption. This focus would have enabled the court to better assess the nature and effects of the power that General Motors exercised. Indeed, one of the most important reasons for protecting privacy is to prevent stifling exercises of power employed to destroy or injure individuals.

Like this, he lists other instances where specific definitions of privacy cause arbitrators to "lose sight of the forest for the trees."[8] He argues,

---

[8] Solove picks apart each of the definitions of privacy but his particular arguments are out of the scope of this paper. We are simply interested in summarizing his work and agreeing that we need to take a different approach than finding a narrow definition of privacy. Two of his other arguments are summarized below:

1. The conception of privacy as intimacy fails to capture the problem in the context [of information about individuals in corporate databases] because for the most part, databases do not invade or disrupt our intimate lives. Our names, addresses, types of cars we own, and so on are not intimate facts about our existence, certainly not equivalent to our deeply held secrets or carefully guarded diary entries. In cyberspace, most of our relationships are more like business transactions than intimate interpersonal relationships.
2. The conception of privacy as control over information only partially captures the problem. The problem is also engendered by the process by which the information is collected, processed, and used-a process which itself is out of control. In other words, what makes this problem significant is the fact that this information is aggregated, that it can be used to make important decisions about people's lives, that it is often subjected to a bureaucratic process lacking much discipline and control, and that the individual has scant knowledge of how the information is processed and used.

To understand his arguments in greater detail, refer to his paper "Conceptualizing Privacy" in the References section at the end of this paper.

> Therefore existing conceptions of privacy have not adequately accounted for this problem. The problem can be better understood and dealt with by conceptualizing privacy from the bottom up, beginning with the problem itself rather than trying to fit the problem into a general category.

He thus prefers to "develop a pragmatic approach to conceptualizing privacy, seeking to understand privacy in terms of practices. By 'practices,' [he is] referring to activities, customs, norms, and traditions[—Therefore, he says] we should explore what it means for something to be private contextually by looking at particular practices, [throughout human history]."

His approach to "conceptualizing privacy draws from a few recurring ideas of pragmatist philosophy: a recognition of context and contingency, a rejection of *a priori* knowledge, and a focus on concrete practices". Keeping this in mind, he favors "an 'approach' to understanding privacy rather than a definition or formula for privacy. [An approach] does not describe the sum and substance of privacy but provides guidance in identifying, analyzing, and ascribing value to a set of related dimensions of practices."

Though we conducted our inquiry of the relationship between privacy and technology by using Nissenbaum's definition of privacy as control of the flow of information, our approach can be considered similar to the approach Calo and Solove propose. Calo suggests defining privacy with respect to the reactions of privacy advocates to new technologies. Solove's work painstakingly corroborates this suggestion and offers further direction, namely to conceptualize privacy from the "bottom up". He guides one interested in privacy to look at human cultural and political norms throughout history, to understand what things have been guarded as private, and categorize situations where the infringement on these things offer an understanding of what privacy is. Our privacy canaries are just such a "bottom up" characterization of privacy, and our DOITs can structure an "approach" to conceptualizing privacy, rather than providing a direct definition of it, just as Solove advocates.

10 Analyzing our lens Critically

We studied reactions from privacy scholars, legal theorists, and the public to technologies that we considered to have affected privacy. We attempted to abstract away the technology and find, in the reaction, those aspects of the technology that the reactions targeted, as well as those notions of privacy that were considered to be undermined. The aspects became our DOITs, and the notions became our privacy canaries. In this approach, we isolated what we felt were the most important DOITs and canaries. But by no means do we believe that our six DOITs are an exhaustive list of aspects of an information technology that can affect privacy, nor do we believe that our canaries encompass everything that privacy is meant to protect. We could have considered other DOITs like:

Diversity of Channels of Information Transfer. One of the reasons the telephone triggered privacy laws more than the telegraph is because the telephone enjoyed a monopoly over the form of communication it provided in a way the telegraph never did. The telephone was the only means of transferring audio information instantaneously, so it was used that much more widely. The telegraph, though quicker than a letter, certainly wasn't the only way of transferring written information long distances.

Speed at Which Information is Created. On social networking sites, many people voice opinions. The ease of doing so gives the ability to publish instinctive reactions, which the poster might later regret or reverse. However, after posting in a moment of passion, it is very hard to hide that information. Technology concretizes information quickly, and makes it hard to suppress that information. We come near discussing this with our discussion of the prevalence of information, but we still do not fully examine the speed dimension.

The Barrier to using a technology to create or transmit information. Another key difference between the telephone and telegraph is that the latter required an understanding of telegraph codes and operation. To use a telegraph to transfer information meant divulging that information to at least one more person than the desired

recipient, the telegraph operator. The telephone was a dedicated channel between two people, without the need for an operator.

Further, there are aspects of the technologies we considered that we did not study, even though they might have been relevant to privacy. In examining the telephone we didn't consider the privacy implications of other people in the room overhearing telephone conversations that were assumed to be private. We didn't talk about Party Lines, communal telephone lines for entire neighborhoods, where anyone could access the line at any time and listen to what others on the line were saying. We also didn't address the personal information in publications like the Yellow Pages and White Pages that carried people's addresses and telephone numbers. In discussing GPS, we didn't address Geographic Information System, Crime Mapping or Cyberstalking, all location based technologies that transfer personal information about people.

Our approach doesn't encompass everything that privacy entails. We strictly discuss only what technology can tell us about privacy. We do not, for example, address what war, children's activities or the relationship between employees and employers can tell us about privacy.

Finally, we don't rigorously defend our lens by defending against a case where a dimension of some technology that is considered one of our DOITs has no bearing at all on privacy. We also don't talk about privacy laws that came from other processes, completely unrelated to our lens. If we were to conduct such a defense we could do so by taking the opposite approach: survey legal cases that alleged particular types of privacy violations (e.g. a privacy tort, a 4th Amendment violation, etc.) and systematically categorize them by the type of technology at issue, or whether there was no technology at issue. That would be a definitive way of mapping the role of different technologies in privacy law, and isolating those parts of privacy law that have developed quite independently of technology.

11 Conclusion

In this thesis we set out to understand what it is about technology and privacy that causes them to be interwoven. We proposed six dimensions of information technology that cause information technology to affect privacy, and we examined each with respect to actual technologies. To enhance our understanding of privacy, we examined what has always been considered private in society, and we tried to address how information technology infringed upon this. We learned that reputation and independence of thought are two important values of privacy that society continues to protect, as new technologies continue to create situations in which these things might be undermined.

12 References

[1] ""Right to Be Forgotten" and Online Search Engines Ruling." "Right to Be Forgotten" and Online Search Engines Ruling - European Commission. N.p., 06 Mar. 2014. Web. 21 May 2017. Accessed at http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

[2] "George Eastman And His Invention, The Kodak Camera." (n.d.). Retrieved March 26, 2017, from http://inventors.about.com/od/estartinventors/ss/George_Eastman.htm

[3] "In 1905 a Third of Households Owned a Camera and Professional Photographers Hated It." *The Phoblographer*. N.p., 28 Aug. 2014. Web. 21 May 2017.

[4] "Should the US Adopt the Right to be Forgotten Online". *Intelligence Squared US*. N.p., 08 Aug. 2015. Web. 21 May 2017. Accessed at http://www.intelligencesquaredus.org/debates/us-should-adopt-right-be-forgotten-online

[5] "Your prescription painkillers could have a tiny GPS tracker hidden inside." *The Week*. N.p., 01 Oct. 2015. Web. 14 Apr. 2017.

[6] 47 U.S. Code § 220 - Accounts, records, and memoranda. (n.d.). Retrieved March 26, 2017, from https://www.law.cornell.edu/uscode/text/47/220

[7] 47 U.S. Code § 222 - Accounts, records, and memoranda. (n.d.). Retrieved March 26, 2017, from https://www.law.cornell.edu/uscode/text/47/222

[8] Anderson, Nate. ""Anonymized" Data Really Isn't—and Here's Why Not." *Ars Technica*. N.p., 08 Sept. 2009. Web. 21 May 2017. Accessed at https://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/

[9] Baio, Andy. "Think You Can Hide, Anonymous Blogger? Two Words: Google Analytics." *Wired. Conde Nast*, 15 Nov. 2011. Web. 21 May 2017. Accessed at https://www.wired.com/2011/11/goog-analytics-anony-bloggers/

[10] Barth, A., Datta, A., Mitchell, J., & Nissenbaum, H. (2006). Privacy and contextual integrity: framework and applications. 2006 IEEE Symposium on Security and Privacy (S&P'06). doi:10.1109/sp.2006.32

[11] Black, Ken. Business statistics: contemporary decision making. Cincinnati, OH: South-Western College Pub., 2001. Print.

[12] Blackstone, W. Commentaries on the Laws of England (1916). Volume 2. Bancroft-Whitney. Harvard University. Digitized May 8, 2008 (Google Book: https://books.google.com/books?id=R20aAAAAYAAJ&dq=blackstone+eavesdropping+commentaries+ch+13&source=gbs_navlinks_s)

[13] Breach of confidence. Office of the Information Commissioner Queensland. N.p., n.d. Web. 21 May 2017. Accessed at https://www.oic.qld.gov.au/annotated-legislation/rti/schedule-3/8-information-disclosure-of-which-would-found-action-for-breach-of-confidence/section-81/breach-of-confidence

[14] Burn-Murdoch, John. "UK technology firm uses machine learning to combat gambling addiction." *The Guardian*. 01 Aug. 2013. Web. 21 May 2017. Accessed at https://www.theguardian.com/news/datablog/2013/aug/01/uk-firm-uses-machine-learning-fight-gambling-addiction

[15] California Penal Code - PEN § 646.9. Findlaw. N.p., n.d. Web. 13 Apr. 2017.

[16] Calo, Ryan. "The Drone as Privacy Catalyst." *Stanford Law Review*. N.p., 13 July 2016. Web. 21 May 2017. Accessed at https://www.stanfordlawreview.org/online/the-drone-as-privacy-catalyst/

[17] Campanile, Carl. "Cornell dean says ISIS welcome on campus in undercover video." *New York Post*. 25 Mar. 2015. Web. 21 May 2017. Accessed at http://nypost.com/2015/03/24/cornell-dean-says-isis-welcome-on-campus-in-undercover-video/

[18] *Cardwell v. Lewis 417 U.S. 583 (1974)*. Justia Law. N.p., n.d. Web. 13 Apr. 2017.

[19] Casetext. N.p., n.d. Web. 13 Apr. 2017.

[20] Christin, Angèle. "From Daguerreotypes to Algorithms." ACM SIGCAS Computers and Society 46.1 (2016): 27-32. Web. Accessed at http://www.angelechristin.com/wp-content/uploads/2014/06/Daguerreotypes-pdf.pdf

[21] Communications Act of 1934. (n.d.) Retrieved March 26, 2017, from https://transition.fcc.gov/Reports/1934new.pdf

[22] Communications Assistance for Law Enforcement Act. (2017, March 17). Retrieved March 26, 2017, from https://en.wikipedia.org/wiki/Communications_Assistance_for_Law_Enforcement_Act

[23] Dash, Samuel, Schwartz, Richard and Knowlton, Robert. *The Eavesdroppers* (1959). Rutgers University Press, 1959.

[24] Diffie, W. and Landau, S. E. *Privacy on the line: the politics of wiretapping and encryption* (2010). Cambridge, MA: MIT Press.

[25] Digital Media Law Project. (n.d.). Retrieved March 26, 2017, from http://www.dmlp.org/legal-guide/illinois-false-light

[26] *Douglass v. Hustler Magazine, Inc*. H2O. N.p., n.d. Web. 21 May 2017. Accessed at https://h2o.law.harvard.edu/cases/424

[27] Expungement and Criminal Records: State-Specific Information. Findlaw. N.p., n.d. Web. 21 May 2017. Accessed at http://criminal.findlaw.com/expungement/expungement-and-criminal-records-state-specific-information.html

[28] FDR Message to Congress Asking to Create FCC. N.p., n.d. Web. 21 May 2017. Accessed at http://newdeal.feri.org/timeline/1934g2.htm

[29] FindLaw's United States Supreme Court case and opinions. (n.d.). Retrieved March 26, 2017, from http://caselaw.findlaw.com/us-supreme-court/96/727.html

[30] Fischer, C. S. *America Calling: A Social History of the Telephone to 1940* (1992). University of California Press.

[31] George Eastman Biography. *Encyclopedia of World Biography*. N.p., n.d. Web. 21 May 2017. Accessed at http://www.notablebiographies.com/Du-Fi/Eastman-George.html

[32] Godkin, E.L. "The Rights of the Citizen to his own reputation". *Scribner's Magazine*, Volume 8. Ed. Edward Livermore Burlingame, Robert Bridges, Alfred Dashiell. Harlan Logan Publisher. Charles Scribners Sons, 1890 Original from the University of Michigan. Digitized Aug 1, 2005 (Google Book: https://books.google.com/books?id=KsACAAAAMAAJ)

[33] Gregson, Christine, B. "California's Antistalking Statute: The Pivotal Role of Intent". 28 *Golden Gate U. L. Rev*. (1998). http://digitalcommons.law.ggu.edu/ggulrev/vol28/iss2/4

[34] Head, J.W. & Cooper, and W.F., *Tennessee Reports: Reports of Cases Argued and Determined in the Supreme Court of Tennessee* (1904). Volume 40. G.I. Jones, UC Southern Regional Library Facility. Digitized Apr 17, 2015 (Google Book: https://books.google.com/books?id=W1NIAQAAMAAJ&dq=a+person+who+secretly+and+stealthily+approaches+near+to+the+room&source=gbs_navlinks_s)

[35] Hill, K. "The Technologies Are New; The Privacy Fears Aren't" (2012, January 10). Retrieved March 26, 2017, from https://www.forbes.com/sites/kashmirhill/2012/01/10/the-technologies-are-new-the-privacy-fears-arent/#27b8b1982ae7

[36] Kant, Immanuel. "What Is Enlightenment". N.p., n.d. Web. 21 May 2017. Accessed at http://www.columbia.edu/acis/ets/CCREAD/etscc/kant.html

[37] Kaplan, D. A. "Suspicions and Spies in Silicon Valley" (2010). Retrieved March 26, 2017, from http://www.newsweek.com/suspicions-and-spies-silicon-valley-109827

[38] Mill, John Stuart. *On Liberty*. London: Penguin, 2010. Print.

[39] Mosbergen, Dominique. "Indian Women Arrested Over Facebook Post Questioning Mumbai's 'Bal Thackeray Shutdown'" *The Huffington Post*. 19 Nov. 2012. Web. 21 May 2017. Accessed at http://www.huffingtonpost.com/2012/11/19/india-facebook-arrest-women-post-questioning-mumbai-bal-thackeray-shutdown_n_2159307.html

[40] *Nardone v. United States 308 U.S. 338* (1939). Justia Law. N.p., n.d. Web. 21 May 2017.

[41] Negley, Glenn. "Philosophical Views on the Value of Privacy." *Law and Contemporary Problems* 31.2 (1966): 319. Web.

[42] New York Consolidated Laws, Civil Rights Law § 50. Findlaw. N.p., n.d. Web. 21 May 2017. Accessed at http://codes.findlaw.com/ny/civil-rights-law/cvr-sect-50.html

[43] Radio Act of 1927. (n.d.). Retrieved March 26, 2017, from http://earlyradiohistory.us/1927act.htm

[44] Rosenzweig, M. L. (1947). “Law of Wiretapping”. *Cornell Law Review* 33(1)

[45] Sarvas, Risto, Frohlich, David M. “From Snapshots to Social Media - The Changing Picture of Domestic Photography Computer Supported Cooperative Work”. (2011) *Springer Science & Business Media*. (Google book: https://books.google.com/books?id=0N-hMblACNAC)

[46] Seipp, David. *The Right to Privacy in American History* (1977). Program in Information Resources Policy, Harvard University, Cambridge, Massachusetts, June.

[47] Solove, Daniel J. “Conceptualizing Privacy” (2002). *California Law Review* 90.4: 1087. Web.

[48] Spears, V.P. “The Case That Started It All: Roberson v. The Rochester Folding Box Company” (2008). *Privacy & Data Security Law Journal.*

[49] Ted. “Ted’s Photographics - The History of Photography - Photographs In Print”. N.p., n.d. Web. 21 May 2017. Accessed at http://www.ted.photographer.org.uk/photohistory_inprint.htm

[50] *The history and growth of the United States census*. (1900). United States. Bureau of Labor

[51] The History of the Telegraph. (n.d.). Retrieved March 26, 2017, from http://www.personal.psu.edu/jtk187/art2/telegraph.htm

[52] The Right to Privacy. (n.d.). Retrieved March 26, 2017, from http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[53] The Trial of John Peter Zenger. (n.d.). Retrieved March 26, 2017, from http://www.ushistory.org/us/7c.asp

[54] Thompson, Clive. “The Invention of the “Snapshot” Changed the Way We Viewed the World.” *Smithsonian Institution*, 01 Sept. 2014. Web. 21 May 2017. Accessed at http://www.smithsonianmag.com/innovation/invention-snapshot-changed-way-we-viewed-world-180952435/

[55] U.S. Const. Amend. IV.

[56] Understanding the 1890 Warren and Brandeis "The Right to Privacy" Article. (n.d.). Retrieved March 26, 2017, from https://nationalparalegal.edu/UnderstandingWarrenBrandeis.aspx?AspxAutoDetectCookieSupport=1

[57] United States Updates Global Positioning System Technology. N.p., n.d. Web. 14 Apr. 2017.

[58] *United States v. Van Leeuwen 397 U.S. 249* (1970). Justia Law. N.p., n.d. Web. 21 May 2017. Accessed at https://supreme.justia.com/cases/federal/us/397/249/case.html

[59] Veeder, V. V. *The History and Theory of the Law of Defamation* (1903). I. Columbia Law Review, 3(8), 546. doi:10.2307/1109121

[60] Vega, Tanzina. "Congress Hears From Apple and Google on Privacy." *The New York Times*. 10 May 2011. Web. 21 May 2017. Accessed at https://mediadecoder.blogs.nytimes.com/2011/05/10/congress-hears-from-apple-and-google-on-privacy/?_r=0

[61] Voyeurism Statutes 2009. Accessed on 04/13/2017 at http://www.ndaa.org/pdf/voyeurism_statutes_mar_09.pdf

[62] Waddams, S. M. *Dimensions of Private Law: Categories and Concepts in Anglo-American Legal Reasoning* (2003). Cambridge University Press. (Google Book: https://books.google.com/books?id=niVM2zzSUMQC)

[63] "Wiretapping: The State Law" (1961). *The Journal of Criminal Law, Criminology, and Police Science*, Vol. 51, No. 5 pp. 534-544

[64] Wnyw. "Hidden GPS devices to track suspects raise legal concerns." *WNYW*. N.p., n.d. Web. 14 Apr. 2017.

[65] Zhu, R. "Distinguishing the Public from the Private: Aristotle's Solution to Plato's Paradox". *History of Political Thought* 25.2 (2004): 231-242. Web.