Information Privacy Law

Joseph Mornin
Berkeley Law School
joseph@mornin.org

Fall 2013
Prof. Schwartz

Contents

§ 1 Very Short Overview

1.1 Privacy and the Media

1. **Torts and the First Amendment**: PLF p. 52.
2. **Information gatheriing**: intrusion upon seclusion, paprazzi, video voyeurism.
3. **Disclosure of truthful information**: public disclosure of private facts, newsworthiness, First Amendment limitations,
4. **Dissination of false or misleading information**: defamation, false light, infliction of emotional distress.
5. **Appropriation of name or likeness**: appropriation, right of publicity, noncommercial use, imitators.

1.2 Privacy and Law Enforcement

1. **Fourth Amendment**: wiretapping, bugging, REOP, third party doctrine, open fields/curtilage, canine sniffs.
2. **Surveillance**: § 605, Title III, ECPA, CALEA.
3. **Digial searches and seizures**: computer searches, email/*Warshak*, Internet metadata collection, keylogging.
4. **National security and foreign intelligence**: balancing privacy and speech, FISA, emergency exceptions, the wall.

1.3 Health Privacy

1. **Confidentiality of medical information**: HIPAA (privacy and security rules), HITECH Act.
2. **Constitutional protection of medical information**: informational/decisional, constitutional torts, compelling state interest in disclosure, *Westinghouse* balancing factors.
3. **Genetic information**: state regulations, future diary, cheek swabs of arrestees.

1.4 Privacy and Government Records

1. **Public access to government records**: public court records, pseudonymous litigation, FOIA/exemptions, arrest records, police reports, Megan's Law.
2. **Government records of personal information**: Fair Information Practices, Privacy Act, DPPA.

1.5 Privacy of Financial and Commercial Data

1. **Financial services industry**: FCRA, "consumer report," GLB Act, identity theft.
2. **Commercial entities**: selling data, stalking, FTC safeguards, VPPA, COPPA, defining PII.
3. **Data security**: breach notification laws, actual harm, FTC enforcement.

1.6 International Privacy Law

1. **OECD guidelines**.
2. **European privacy protection**: personal sovereignty vs. dignity, ECHR 8, "wide margin of appreciation," EU data protection directive.

§ 2 Overview

2.1 Privacy and the Media

1. **Torts and the First Amendment**: see PLF p. 52.
2. **Information gathering**.
   (a) **Intrusion upon seclusion**.
      i. Occurs when one (1) **intrudes** (2) if the intrusion would be **highly offensive** to a reasonable person. *Nader v. GM.*
      ii. People can reasonably expect to exclude eavesdropping reporters from their **homes**. The First Amendment does not justify or excuse the tort. *Dietemann v. Time.*
      iii. **Professionals** assume the risk that their clients will publicize their interactions. *Desnick v. ABC.* The Court distinguished *Dietemann*: "Dietemann was not in business, and did not advertise his services or charge for them. His quackery was private."[1]
      iv. **News reporting** does not justify highly offensive intrusions. *Shulman v. Group W.*
   (b) **Paparazzi**.
      i. "[c]rimes and torts committed in news gathering are not protected. There is no threat to a free press in requiring its agents to act within the law . . . ."[2] *Galella v. Onassis.*
      ii. California Anti-Paparazzi Act—see p. 34.
   (c) **Video Voyeurism Prevention Act**: prevents intentionally capturing images of intimate areas under circumstances (1) where the person believed he could disrobe in privacy or (2) where intimate areas would not be visible to the public.[3]
3. **Disclosure of truthful information**.
   (a) **Key questions**: when should disclosure trigger civil liability? How can liability coexist with the First Amendment?
   (b) **Public disclosure of private facts**.
      i. Liability exists when the matter publicized is (1) **highly offensive** and (2) **not of legitimate concern to the public**.[4] Seven states don't recognize it.
      ii. "There can be no privacy in that which is **already public**."[5] *Gill v. Hearst.* Publishing to a wider audience doesn't matter (but the dissent disagrees).

[1] Casebook p. 90.
[2] Casebook p. 100.
[3] Casebook pp. 107–108.
[4] Casebook p. 110.
[5] casebook p. 111.

iii. **Involuntary public exposure** does not negate privacy protections. *Daily Times Democrat v. Graham.*

iv. What are the boundaries of "the public"? Can it be a small group? *Miller v. Motorola.* The court here held that "the public disclosure requirement may be satisfied by proof that the plaintiff has a special relationship with the 'public' to whom the information is disclosed," but many courts disagree.[6]

v. There is no liability for disclosing facts that are (1) not private and (2) newsworthy. *Sipple v. Chronicle.*

vi. **Three tests for newsworthiness** (see p. 38):

A. **Defer to editorial judgment** and make no distinction between news and entertainment. (See *Shulman*, p. 4.2.1.7, holding that the test is "substantial relevance" to a newsworthy subject.)

B. Look to the **"customs and conventions of the community."**

C. Require a **"logical nexus"** between the person and the matter of legitimate public interest. (See *Bonome v. Kaysen.*)

(c) **First Amendment limitations.**

i. States can't prohibit the accurate publication of a **name obtained from public records**. *Cox v. Cohn.*

ii. **Pseudonymous litigation**: "[I]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."[7] *Florida Star v. B.J.F.*

iii. " . . . **a stranger's illegal conduct** does not suffice to remove the First Amendment shield from speech about a **matter of public concern** [but only for matters of public concern—not general conversations]." *Barnicki v. Vopper.*

4. **Dissemination of false or misleading information**.

(a) **Defamation**:

i. Defined as **false information** that **harms the reputation** of the victim. Consists of libel (written) and slander (spoken).

ii. Computer service providers are not publishers (a category which includes distributors). Also, CDA § 230 did not create notice-based liability for service providers. *Zeran v. AOL.*

iii. Does CDA § 230 provide too much immunity from tort liability? **Blumenthal v. Drudge**.

[6] Casebook p. 121.
[7] Casebook p. 155–60.

iv. To recover for defamation, **public officials** must prove **actual malice**—i.e., knowledge that the statement was false or made with reckless disregard for whether it was false or not.

v. **Private citizens do not have to prove actual malice** to recover for actual injuries. However, they have to prove actual malice to recover **punitive damages**, or else juries might punish unpopular views. *Gertz v. Robert Welch.*

vi. Celebrity divorces are not public controversies. *Time v. Firestone.*

vii. People can become **"voluntary limited-purpose public figure[s]"** by injecting themselves into news stories. *Atlanta Journal-Constitution v. Jewell.*

(b) **False light**:

i. Liability if (1) **highly offensive** to a reasonable person and (2) the actor acted with knowledge or reckless disregard of the falsehood.[8] Different from defamation in that **no harm to reputation is necessary**.

ii. For matters of **public concern**, defendants are only liable for the false light tort if they acted with **knowledge of falsity or in reckless disregard for the truth**—i.e., actual malice. *Time v. Hill.* Courts are split on whether the actual malice standard also applies to private citizens (i.e., not public figures).

(c) **Infliction of Emotional Distress**:

i. Liability arises when "**extreme and outrageous conduct intentionally or recklessly** causes severe emotional distress."[9]

ii. To claim intentional infliction of emotional distress from published material, public figures and officials must also show *New York Times* malice. *Hustler v. Falwell.*

iii. There is **special protection** for public speech on matters of **public concern**. *Snyder v. Phelps* (Westboro Baptist).

5. **Appropriation of name or likeness**.

(a) Appropriation: **privacy-based**; concerned with dignity.

(b) Right of publicity: **property-based**; concerned with commercial reward.[10]

(c) Appropriation of identity can occur without using a name or likeness—e.g., a **catchphrase** like "Here's Johnny!" *Carson v. Here's Johnny.* Courts have interpreted "likeness" broadly.

[8] Casebook p. 205.
[9] Casebook p. 211.
[10] Casebook p. 221.

(d) The tort of appropriation **does not apply to noncommercial use**. *Raymen v. United Senior Association*. The exception applies to news (*Finger v. Omni*, below), parody, satire, etc. (e.g., the Beach Boys song "Johnny Carson").

(e) **News media** can use a person's name or likeness without incurring liability as long as there is a **"real relationship"** between the person and the story. *Finger v. Omni Publications*. (But what about the fact that most news organizations are also commercial entities?)

(f) Letting a news broadcast show an **entire act** threatens the economic value of the performance. The **First Amendment** doesn't allow news organizations to undermine performers' publicity rights. *Zacchini v. Scripps-Howard*.

(g) **Imitators** are liable under the appropriation tort if they don't add **substantial value**. *Estate of Presley v. Russen*.

2.2 Privacy and Law Enforcement

1. **Fourth Amendment**.
   (a) No privacy in envelope exteriors. *Ex parte Jackson.*
   (b) **Special needs doctrine**: schools, government workplaces, and certain highly regulated business.[11]
   (c) Sobriety checks: ok, because they aim to protect road safety. Drug violation checks: not ok, because aim to detect general criminal wrongdoing.[12]
   (d) *Terry* stops: upon reasonable suspicion.[13]
   (e) **Wiretapping and bugging**.
      i. Early in the 20th Century, the Court read the Fourth Amendment narrowly to exclude protections for phone wiretapping. *Olmstead v. U.S.*
      ii. **Risk theory**: if you break the law, you run the risk that the offer you make in-person "will be accurately reproduced in court by . . . mechanical rendering." *Lopez v. U.S.*
      iii. A search occurs when the government violates a person's reasonable expectation of privacy. *Katz v. U.S.*
      iv. **Undercover agents**: "Inescapably, one contemplating illegal activities must realize the risk that his companions may be reporting to the police." *U.S. v. White.*
   (f) **Reasonable expectation of privacy**.
      i. No REOP in numbers dialed. *Smith v. Maryland.*
      ii. Canine sniffs: sui generis, and not a search. *U.S. v. Place.*
      iii. Canine sniffs during traffic stops are not searches. Government conduct that only reveals the presence of contraband compromises no legitimate privacy interest. *Illinois v. Caballes.* (Souter and Ginsburg dissents: see p. 50.)
      iv. Dogs' certification and training are adequate indications of their reliability. *Florida v. Harris.*
      v. A dog sniff on the front porch of a home is a search because it's a trespass. *Florida v. Jardines.*
      vi. No reasonable expectation of privacy in trash bags left on the street. *California v. Greenwood.*
      vii. **Plain view doctrine**: no expectation of privacy in things that can be seen from a public vantage point.[14]

[11] Casebook p. 252.
[12] Casebook p. 252–53.
[13] Casebook p. 254.
[14] Casebook p. 293.

viii. **Open fields doctrine**: no expectation of privacy in the open fields a person owns—but curtilage is an exception.

ix. Aerial surveillance: no REOP in a backyard viewed from 400 feet. *Florida v. Riley.*

x. No industrial curtilage. *Dow Chemical v. U.S.*.

xi. Thermal imaging: "Where, as here, the government uses a **device that is not in general public use**, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment 'search,' and is presumptively unreasonable without a warrant." *Kyllo v. U.S.*.

2. **Federal electronic surveillance law**.

(a) **Section 605** of the Federal Communications Act, 1934: prevented unauthorized interception or divulgence of communications.[15] Did not apply to state prosecutions or bugging (i.e., non-wire communications).

(b) **Title III** (of the Ombnibus Crime Control and Safe Streets Act of 1968): enacted in 1968 in response to *Katz*; amended in 1986 as the Wiretap Act. Prevented all warrantless federal, state, and private wiretapping, but allowed one-party consent.[16] Excluded wiretaps for national security purposes.

(c) **Electronic Communications Privacy Act**.

i. See Schwartz and Solove, "ECPA in a Nutshell."

ii. Types of communications:[17]

A. **Wire communications**: travel through a wire or similar medium. Must include a human voice.

B. **Oral communications**: typically intercepted through bugs.

C. **Electronic communications**: all non-wire, non-oral communications—e.g., email.

iii. Statutory structure:

A. Wiretap Act.[18]

B. Stored Communications Act.[19]

C. Pen Register Act.[20]

iv. **Video**: if it's oral, it's covered by the Wiretap Act. If it's just silent video, federal electronic surveillance law does not apply.[21]

[15] Casebook p. 313.
[16] Casebook p. 315.
[17] Casebook p. 316.
[18] Casebook p. 317–19.
[19] Casebook p. 319–321.
[20] Casebook p. 322.
[21] Casebook p. 322.

v. Electronic surveillance orders under wiretap law have recently expanded.[22]

vi. State electronic surveillance law: many require consent of all parties to a conversation.

(d) **Communications Assistance for Law Enforcement Act**.

i. Telecom providers must assist legally authorized surveillance.

ii. Networks must be designed to telecoms can intercept communications and provide them to law enforcement.

iii. VoIP qualifies.

3. **Digital searches and seizures**.

(a) **Searching the contents of computers**: third parties have apparent authority to consent to a search when an officer reasonably but erroneously thinks the third-party has authority to consent. *U.S. v. Andrus*.

(b) The Wiretap Act's protection against "interception" does not apply to stored electronic communications. **"Electronic communication" under the Wiretap Act does not include stored data** (so the SCA applies). *Steve Jackson Games v. U.S.S.S.*

(c) Kerr: does the Fourth Amendment protect stored emails?[23]

i. *Internal perspective*: the Internet is a virtual world. Email is analogous to postal mail, so a warrant is required.

ii. *External perspective*: the message passes through a third party. No warrant is required to get email stored with a third party.

(d) There is a Fourth Amendment reasonable expectation of privacy in the contents of emails. The SCA is unconstitutional to the extent that it lets government compel ISPs to turn over email contents without a warrant. (No other circuit has weighed in.) *U.S. v. Warshak*.

(e) Subscribers do not have a REOP in the **subscription data they give to their ISPs**. Moreover, there is **no exclusionary rule in the SCA**—only damages provisions. *U.S. v. Hambrick*.

(f) Suppression is warranted if the government breaks the law to get information from a service provider. *McVeigh v. Cohen*.

(g) The **collection of Internet metadata is constitutionally indistinguishable from pen register collection**. The Pen Register Act does not provide for suppression, so there was no suppression here. *U.S. v. Forrester*.

(h) *U.S. v. Scarfo*: since the keylogger was only activated when the modem was turned off, so it did not "intercept" a wire communication.

[22] Casebook p. 323 ff.
[23] Casebook pp. 348–49.

4. **National security and foreign intelligence**.

   (a) Domestic surveillance for national security risks infringing "privacy of speech," so a warrant is required.[24] (But foreign surveillance for national security purposes may be different.)[25] *Keith* case.

   (b) **FISA**: applies when foreign intelligence gathering is a "significant purpose" of the investigation. (Otherwise, ECPA applies.)[26]

   (c) The emergency FISA exception allows warrantless searches. *Global Relief Foundation v. O'Neil*.

   (d) **The wall**: FISA authorizes retention of evidence that is "evidence of a crime." The crime need not be related to foreign intelligence—as long as foreign intelligence gathering was "a significant purpose" of the investigation. *U.S. v. Isa*.

   (e) As long as a "significant purpose" of the investigation is gathering foreign intelligence, the evidence acquired can be used in a criminal case. *In re Sealed Case*.

[24] Casebook p. 380.
[25] Casebook p. 381.
[26] Casebook p. 385–86.

2.3 Health Privacy

1. **Confidentiality of medical information**.
   (a) **HIPAA**.
      i. Mainly about **portability**.
      ii. **Privacy rule**: casebook pp. 465–68.
      iii. **Security rule**: casebook pp. 468–69.
      iv. **Covered entities**: health plans, clearinghouses, providers.
      v. **Marketing**: authorization is required, but not for the plan's own services and products.
      vi. Covered entities must make **minimum necessary use and disclosures**.
      vii. May disclose to a **business associate** if there are assurances of safeguards.
      viii. CEs must implement three kinds of **safeguards**: administrative, physical, and technical.
   (b) **HITECH Act**:
      i. Facilitates **electronic health records**. Increases penalties and expands security rule to business associates.
      ii. New **data breach notification** requirements if information has been "compromised." Breach notifications are necessary in all situations except those in which the CE or BA shows a low probability that the information has been compromised.

2. **Constitutional protection of medical information**.
   (a) There are two types of privacy interests: **informational** and **decisional**. *Whalen v. Roe*.
   (b) **Constitutional torts**: 42 U.S.C. § 1983 provides civil remedies for constitutional violations. Constitutional violations become tort actions, enabling plaintiffs to win damages and injunctive relief.[27] There must be a **state actor**. Plaintiffs *cannot* directly sue states because of the Eleventh Amendment, but they *can* sue any state or local government official. They can also sue local governments when their policy or custom inflicts the injury.[28]
   (c) Hospital chaplains can't have open access to patient records, but they can know the patient's "basic problem." *Carter v. BMC*.
   (d) To disclose a person's HIV status, the state must show a compelling government interest that outweighs the substantial privacy interest. *Doe v. Borough of Barrington*.

[27] Casebook p. 510–11.
[28] Casebook p. 510–11.

(e) The seven *Westinghouse* factors weight the privacy interest against competing interests. [29] Interest like containing healthcare costs can outweigh individual privacy interests. *Doe v. SEPTA*.

3. **Genetic information**.

(a) At least 18 state genetic privacy statutes.[30]

(b) DNA can be a **"future diary."**[31]

(c) Issues in DNA databases—see casebook pp. 553–59.

(d) Swabbing the cheek of an arrestee to get a DNA sample is reasonable under the Fourth Amendment. *Maryland v. King*—see p. 61.

[29] Casebook p. 520.
[30] Casebook p. 538.
[31] Casebook p. 539.

2.4 Privacy and Government Records

1. **Public access to government records.**

   (a) **Public records and court records**.

      i. Court records are public in all states.

      ii. In civil suits, plaintiffs sometimes cannot remain anonymous. However, judges have discretion. *Doe v. Shakur*.

   (b) **FOIA**.

      i. Transparency of federal documents is the default. Nine exemptions; two for privacy, with a higher threshold for disclosure of law enforcement documents.[32]

      ii. FOIA does not compel disclosure of rap sheets. They have "practical obscurity" and reveal little about **"what the government is up to."** *DOJ v. Reporters Committee*.

      iii. Disclosure outweighs privacy interests only when there is reasonable evidence of **government impropriety**. *NARA v. Favish*.

   (c) **Constitutional limits on public access**.

      i. States can publish arrest records. *Paul v. Davis*.

      ii. " . . . there is no constitutional right to privacy in one's criminal record." *Cline v. Rogers*.

      iii. After *Whalen*, information in police records is not private. *Scheetz v. The Morning Call*.

      iv. Megan's Laws are constitutional. "Megan's Law does not restrict plaintiffs' freedom of action with respect to their families." *Paul P. v. Verniero*.

2. **Government records of personal information.**

   (a) **Fair Information Practices** are the rights and responsibilities associated with the transfer and use of personal information. Typically, they assign rights to individuals and responsibilities to organizations.[33]

   (b) **Privacy Act** (1974).

      i. Enacts FIPs into federal law.[34] Regulates how federal agencies collect and use personal information. Creates a private right of action.

      ii. Hunting rosters are public records under the Privacy Act, and plaintiffs may be able to show that disclosure would have adverse effects. *Quinn v. Stone*.

[32] Casebook p. 643.
[33] Casebook p. 699.
[34] Casebook p. 701.

iii. Under the Privacy Act, plaintiffs must prove some **actual damages** in order to qualify for the minimum statutory award of $1,000. *Doe v. Chao*.

(c) **Driver's Privacy Protection Act**: state DMVs can disclose personal information only with opt-in (with some exceptions).[35]

[35] Casebook p. 754.

2.5 Privacy of Financial and Commercial Data

1. **Financial services industry**.
   (a) **Fair Credit Reporting Act** (1970).
      i. Scope turns on the **definition of "consumer report."** Most reports dealing with consumer credit fall within this definition.[36] Statutory requirements: see casebook pp. 758–65.
      ii. FCRA does not allow the use of credit reports beyond **"legitimate business needs,"** narrowly construed. *Smith v. Bob Smith Chevrolet.*
      iii. Held: credit reporting agencies are not liable if they take **"reasonable procedures to assure maximum possible accuracy."** Liability requires notice of systemic problems or individual defects. *Sarver v. Experian.*
   (b) **Use and disclosure of financial information**.
      i. **Graham-Leach-Bliley Act**.
         A. Protects only **nonpublic personal information** (NPPI)[37]—e.g., first and last name plus any of the following: SSN, driver's license number, credit card number, etc.
         B. Authorizes sharing between **affiliated companies**. Customers must be told about the sharing, but they can't prevent it. ("Affiliated" means it controls, is controlled by, or is under common control with the other.)
         C. Also authorizes sharing with **unaffiliated companies**, but customers must be able to opt out.
         D. Requires an annual privacy notice.
         E. FTC and other agencies are to establish privacy and security regulations for regulated entities.
   (c) **Identity theft**.
      i. Identity Theft Assumption and Deterrence Act: federal, 1998[38]—and more than 40 state laws.
      ii. Solove: the credit system enables identity theft, e.g., by the frequent use of SSNs as identifiers.[39]
      iii. Identity theft is **foreseeable** and preventable, so banks have to implement reasonable and cost-effective means to address it. *Wolfe v. MBNA.*
      iv. Plaintiffs can recover against credit reporting agencies for emotional distress. *Sloane v. Equifax.*

[36] Casebook p. 758.
[37] Casebook p. 780 ff.
[38] Casebook p. 786.
[39] Casebook p. 787–88.

2. **Commercial entities**.

   (a) **Tort**.

      i. **Selling cardholder data** is not actionable as intrusion upon seclusion or appropriation. *Dwyer v. American Express*.

      ii. The risk of criminal misconduct due to stalking and ID theft are **sufficiently foreseeable** to create a **duty on the investigator** to exercise reasonable care in disclosing a third person's information to a client. *Remsberg v. Docusearch*.

   (b) **Contracts and promises**.

      i. **FTC safeguards**.

         A. FTC **Privacy Rule**: must have a clear statement of policy to customers and consumers.

         B. FTC **Safeguards Rule**: must have a written information security plan describing a program to protect customer information.

      ii. **Privacy statements are not contracts.** The company can retain discretion to determine when the information is "relevant" and when "third parties" might need access. *In re Northwest Airlines*.

      iii. Triggers for FTC enforcement:

         A. Inadequate security.

         B. Data breach due to negligence or failure to train employees.

         C. Broken promises.

         D. Retroactive privacy policy changes.

         E. Deceptive data collection.

         F. Inadequate disclosure of data gathering activities.

      iv. FTC and Google Buzz order: see casebook pp. 824–26. Includes the establishment of a **"comprehensive privacy program"** and 20 years of reporting. After the Safari issue, Google agreed to a $22.5 million fine.

   (c) **Statutory regulation**.

      i. **Video Privacy Protection Act**: courts are split on who is liable for possession of improperly released information. See *Dirkes v. Borough of Runnemede* and *Daniel v. Cantell*.

      ii. **COPPA** (1998). **Safe harbor**: no liability if the provider follows guidelines published by an FTC-approved group.[40] After Dec. 2012: tracking of persistent identifiers of children is now a violation of COPPA—even if the site doesn't know the identity of the child.

   (d) **Defining PII**.

[40] Casebook p. 848.

i. We lack a uniform definition.
ii. Three approaches:[41]
   A. Tautological: PII identifies people.
   B. Non-public: any non-public information is personally identifying.
   C. Specific types: list data fields that count as PII.
iii. Paul Ohm: abandon PII.[42]
iv. Solove and Schwartz: identifiability (and risk) is a continuum. More identifiability means more risk.
v. FTC staff report: when is information not "reasonably linkable" to a person?—When companies do not re-identify it.
vi. Takeaway: lots of legal uncertainty about the definition of PII, here and abroad. EU may have broader definitions.
vii. **Zip codes** can be PII. *Pineda v. Williams-Sonoma*.

3. **Data security**.
   (a) Most states have **data breach notification** laws.
   (b) After a breach, "allegations of increased risk of future identity theft" are not sufficient to establish a compensable injury. *Pisciotta v. Old National Bancorp*.
   (c) FTC can take enforcement actions for inadequate security.

[41] Casebook p. 873.
[42] Casebook p. 877.

2.6 International Privacy Law

1. **OECD guidelines**.
   (a) U.S. is a member.[43]
   (b) Enacted 1980. Grew out of a need for greater interoperability among international privacy frameworks.
   (c) Guidelines are **not binding anywhere**.
   (d) Guidelines:
      i. Collection limitation.
      ii. Data quality.
      iii. Purpose specification.
      iv. Use limitation.
      v. Security safeguards.
      vi. Openness/transparency.
      vii. Individual participation.
      viii. Accountability.
   (e) 2013: OECD adopts a revised recommendation.
   (f) Accountability requires a "privacy management program."
   (g) Notification is required for significant data breaches that are likely to have adverse effects.
2. **Privacy protection in Europe**.
   (a) **Two western cultures of privacy**:
      i. United States: freedom from governmental intrusion; personal sovereignty—e.g., no national ID system.[44]
      ii. Europe: personal dignity, respect, honor, face-saving—e.g., no intrusive credit reports.
   (b) **ECHR Article 8**.
      i. There is a distinction between reporting facts and reporting intimate details. *Von Hannover v. Germany.*
      ii. States have a **"wide margin of appreciation"** in deciding how to "respect" Article 8. They can strike their own balance between privacy protections and freedom of expression. Here, there was no need for a press pre-notification requirement.
   (c) **The European Union Data Protection Directive** (1995).
      i. "Data protection law" (EU) = "information privacy law" (US).
      ii. Goals:

[43] Casebook p. 1063–65 ff.
[44] Casebook p. 1065–70.

   A. Free flow of information.
   B. Protect fundamental rights.
   C. Protect EU citizens' privacy worldwide.

iii. Has shaped privacy law worldwide; the US is an outlier.

iv. Emphases (i.e., FIPs):
   A. Limits on collection.
   B. Data quality principle.
   C. Notice, access, and correction rights for individuals.
   D. EU exclusive ideas:
      - Must have a legal basis to process information (inverse of US approach)—though consent can form a legal basis.
      - Regulation by an independent data protection authority.
      - Restrictions on data exports.
      - Limits on automated decisionmaking.
      - Additional protections for sensitive data.

v. Allows data export only to countries with adequate protections. The **US does not have adequate protection** according to the EU.

vi. Possible EU–US solutions:
   A. Safe harbor standards that US companies could voluntarily follow.
   B. Model contractual clauses. (Don't reinvent the wheel. Mental economy.)
   C. Binding corporate rules.

§ 3 Introduction to Information Privacy Law

3.1 Information Privacy, Technology, and the Law

3.1.1 Involuntary Public Figures and Public Interest: *Sidis v. F-R Publishing Corp.*

1. Sidis, a former child prodigy, sued F-R over a *New Yorker* story by Thurber about his current life. The court held that the lives of public figures are matters of public concern, so lower privacy protections apply.[45]

3.2 Information Privacy Law: Origins and Types

3.2.1 Common Law

3.2.1.1 The Right to Be Let Alone: Warren and Brandeis, *The Right to Privacy*

1. In response to advances in media (e.g., gossip) and technology (e.g., the Kodak Brownie), which can cause "mental pain and distress, far greater than could be inflicted by mere bodily injury."[46]

2. Defamation doesn't protect "injury to the feelings."[47]

3. Intellectual property protections—for instance, the right to prevent publication—are part of a broader common law right to privacy.[48]

4. There is a "general right of the individual right of the individual to be let alone."[49] Invasion of privacy is a common law tort.[50]

5. Protections don't apply to public figures (at least, not to public officials—protections *do* apply to "modest and retiring individuals," so an involuntary public figure like Sidis would probably have a cause of action).[51]

3.2.1.2 Four Privacy Torts: Prosser, *Privacy*

1. Intrusion.[52]

2. Disclosure.

3. False light.

4. Appropriation.

[45] Casebook pp. 5–6.
[46] Casebook p. 14.
[47] Casebook p. 15.
[48] Casebook pp. 15–16.
[49] Casebook p. 18.
[50] Casebook pp. 18-20.
[51] Casebook p. 21.
[52] Casebook p. 27.

3.2.1.3 Adopting the Prosser Torts: *Lake v. Wal-Mart Stores, Inc.*

1. Joining most other states, Minnesota adopted the Prosser privacy torts (except false light, because it is too close to defamation and because it raises First Amendment concerns).[53]

3.2.1.4 Privacy and Other Areas of Law

1. Torts: Prosser's four, breach of confidentiality, defamation, infliction of emotional distress.
2. Evidence: privileged relationships.
3. Property: trespass. Also, should we treat personal information as property?
4. Contract: private agreements.
5. Criminal law: injury (to body and property), trespass, stalking/harassing, blackmail, wiretapping, identity theft.

3.2.2 Constitutional Law

1. Federal: First Amendment (anonymous speech), Third (privacy of the home), Fourth (many interpretations), Fifth (privilege against self-incrimination). *Griswold* (marital privacy), *Whalen* ("constitutional right to information privacy").
2. State: many state constitutions (e.g., California) have explicit privacy protections.

3.2.3 Statutory Law

1. Federal: many specific statutes.[54] Also, the general Privacy Act of 1974.
2. State: many specific statutes, but less than a third have enacted "omnibus data protection laws."[55]

3.2.4 International Law

1. OECD guidelines, APEC Privacy Framework.[56]

[53] Casebook pp. 29–31.
[54] See casebook pp. 36–39.
[55] Casebook p. 39.
[56] Casebook pp, 39–40.

3.3 Perspectives on Privacy

3.3.1 Philosophy

3.3.1.1 The Concept of Privacy and the Right to Privacy

1. The *concept* of privacy is distinct from the *right* to privacy.

3.3.1.2 The Public and Private Spheres

1. Arendt, Mill.[57].

3.3.2 Definition and Value

3.3.2.1 Westin, *Privacy and Freedom*

1. Surveillance is necessary in order to enforce social norms.
2. Four states of privacy: solitude, intimacy, anonymity, reserve.
3. Functions of privacy: personal autonomy, self evaluation, limited and protected communication.[58]

3.3.2.2 Cohen, *Examined Lives: Informational Privacy and the Subject as Object*

1. Autonomy requires a zone of insulation from scrutiny and interference.
2. " . . . the experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behavior."[59]

3.3.2.3 Solove, *Conceptualizing Property*

1. "When we state that we are protecting "privacy," we are claiming to guard against disruptions to certain practices."[60]
2. Privacy depends on context; there is no common denominator.[61]
3. Reductionists: privacy can be reduced to other concepts and rights.[62]

3.3.2.4 Allen, *Coercing Privacy*

1. Privacy is a "foundation, a precondition of a liberal egalitarian society."[63] So we should sometimes force it on people—for instance, through public nudity laws.

[57] Casebook pp. 40–41.
[58] Casebook pp. 42–45.
[59] Casebook pp. 48-49.
[60] Casebook p. 52.
[61] Casebook p. 53.
[62] Casebook p. 54.
[63] Casebook p. 55.

3.3.2.5 Schwartz, *Privacy and Democracy in Cyberspace*

1. Control over information is a flawed understanding of privacy in digital contexts. For instance, it assumes we are autonomous, but we often are not—for instance, if we accept a boilerplate EULA that allows the company to do anything with our information.[64]

3.3.2.6 Simitis, *Reviewing Privacy in an Information Society*

1. Personal information can enforce standards of behavior, which means that increased surveillance can facilitate "adjustment" but that it may be harmful to democracy.[65]

3.3.3 Critics

3.3.3.1 Posner, *The Right of Privacy*

1. Gossip can inform. Many people present themselves deceptively, so nosiness can be helpful.[66]

3.3.3.2 Cate, *Principles of Internet Privacy*

1. U.S. law historically has a strong preference for the free flow of information, which has "significant economic and social benefits" (e.g., price signals).[67]

2.

3.3.4 Feminism and Privacy

3.3.4.1 Privacy as Gender Oppression: *State v. Rhodes*

1. Should a husband be convicted for whipping his wife? No—family privacy outweighs the need to punish impulsive violence.

3.3.4.2 Siegel, *"The Rule of Love": Wife Beating as Prerogative and Privacy*

1. *Rhodes* is one of many cases in which privacy serves as a tool of gender oppression.[68]

3.3.4.3 MacKinnon, *Toward a Feminist Theory of the State*

1. Privacy can perpetuate subordination.[69]

[64] Casebook p. 57.
[65] Casebook pp. 59–61.
[66] Casebook pp. 62–63.
[67] Casebook pp. 66–68.
[68] Casebook pp. 72–74.
[69] Casebook pp. 74–75.

3.3.4.4 Allen, *Uneasy Access: Privacy for Women in a Free Society*

1. MacKinnon goes too far. Privacy is not an inherent threat to women. We should seek "adequate and meaningful privacy . . . "[70]

[70] Casebook pp. 75–76.

§ 4 Privacy and the Media

4.1 Information Gathering

4.1.1 Intrusion upon Seclusion

4.1.1.1 Restatement (Second) of Torts § 652(b): Intrusion upon Seclusion

1. Occurs when one (1) **intrudes** (2) if the intrusion would be **highly offensive** to a reasonable person.

4.1.1.2 Unreasonable Intrusion: *Nader v. General Motors Corp.*

Information gathering becomes actionable when the information sought is confidential and the conduct is unreasonably intrusive.[71] Here, the unreasonable behavior was eavesdropping/wiretapping and possibly overzealous surveillance.

1. GM harassed and eavesdropped on Nader after he published *Unsafe at Any Speed*. Nader sued for intrusion upon seclusion.
2. Two causes of action were not actionable as intrusions upon seclusion (entrapping him with girls, making threatening or harassing phone calls), but two were (wiretapping, overzealous public surveillance).
3. Information gathering becomes actionable when the information sought is confidential and the conduct is unreasonably intrusive.[72]
4. Held: Nader's allegations were sufficient to withstand a motion for summary judgment.[73]
5. The case later settled, and Nader won massive publicity.
6. Justice Brietel, concurring: courts should consider allegations together, since privacy invasions can occur through "extensive or exhaustive monitoring and cataloguing of acts normally disconnected and anonymous."[74]

4.1.1.3 Private Spaces, Eavesdropping Reports, and the First Amendment: *Dietemann v. Time, Inc.* People can reasonably expect to exclude eavesdropping reporters from their homes. The First Amendment does not justify or excuse the tort.

1. Dietemann was practicing quack medicine in his home (cf. *Desnick* below). A Time reporter secretly recorded a session and later published a story.

[71] Casebook p. 81.
[72] Casebook p. 81.
[73] Casebook p. 82.
[74] Casebook p. 83.

2. The court held that Dietemann's "den was a sphere from which he could reasonably expect to exclude eavesdropping newsmen." He shouldn't expect that everything said in his home will be "transmitted by photograph or recording, in our modern world, in full living color and hi-fi to the public at large . . . ."[75]

3. Time attempted a First Amendment defense, but the "First Amendment has never been construed to accord newsmen immunity from torts or crimes committed during the course of newsgathering."[76]

4.1.1.4 Public vs. Spaces: *Desnick v. American Broadcasting Co., Inc.*

Professionals assume the risk that their clients will publicize their interactions. The Court distinguished *Dietemann*: "Dietemann was not in business, and did not advertise his services or charge for them. His quackery was private."[77]

1. ABC did a show about fraudulent eye surgery involving Desnick, a surgeon.

2. The court held that although ABC had engaged in undercover surveillance, there was no privacy violation because there was no invasion of a space that the tort of trespass seeks to protect. It distinguished *Dietemann*: "Dietemann was not in business, and did not advertise his services or charge for them. His quackery was private."[78]

4.1.1.5 Newsorthiness and Offensiveness: *Shulman v. Group W Productions, Inc.*

"[T]he fact that a reporter may be seeking 'newsworthy' material does not in itself privilege the investigatory activity."[79] A jury here could find that the recording was highly offensive.

1. Ruth Shulman was airlifted from a car accident. The ordeal was filmed for a TV show, including a cameraman in the helicopter and a microphone attached to the nurse's shirt which recorded the details of their conversations.[80]

2. Upon broadcast, Shulman sued for unlawful intrusion and public disclosure of private facts.

[75] Casebook p. 87.
[76] Casebook p. 87.
[77] Casebook p. 90.
[78] Casebook p. 90.
[79] Casebook p. 97.
[80] Casebook pp. 94–96.

3. The trial court granted summary judgment because it found that the events were newsworthy.

4. Intrusion has two elements: (1) intrusion (2) that is highly offensive.

5. The court found (1) that Shulman had a reasonable expectation of privacy in the helicopter ride and in her conversations with the nurse, and (2) a jury could find that the recording was highly offensive.

6. The defendants' conduct was not privileged. "[T]he fact that a reporter may be seeking 'newsworthy' material does not in itself privilege the investigatory activity."[81]

7. Reversed.

4.1.2 Paparazzi

4.1.2.1 Torts and Paparazzi: *Galella v. Onassis*

"[c]rimes and torts committed in news gathering are not protected. There is no threat to a free press in requiring its agents to act within the law . . . ."[82]

1. Galella was a famously annoying paparazzo who had frequent run-ins with Onassis and her family.

2. Galella sued Onassis for false arrest, malicious prosecution, and other causes of action. Onassis counterclaimed for invasion of privacy, among others.[83]

3. Galella did not seriously dispute the tort claims. The court dismissed his First Amendment arguments—"[c]rimes and torts committed in news gathering are not protected. There is no threat to a free press in requiring its agents to act within the law . . . ."[84]

4.1.2.2 California Anti-Paparazzi Act: Cal. Civ. Code § 1708.8

1. The Act defines **two forms of invasion of privacy**:[85]
   (a) **Physical** invasion.
   (b) **Constructive** invasion (using tools to capture information that would not have been available without trespsass).

2. No punishment for the sale or dissemination of recordings in violation of the Act.[86]

[81] Casebook p. 97.
[82] Casebook p. 100.
[83] Casebook p. 99.
[84] Casebook p. 100.
[85] Casebook p. 101.
[86] Casebook p. 102.

3. 2005 amendment: prohibited assault committed with the intent to capture information in violation of the Act.
   (a) One criticism: assault is an intentional tort, so this doesn't apply if the paparazzi act negligently.
4. 2009 amendment: prohibited sale or dissemination if the person knows the information was captured in violation of the law.
   (a) But media buyers may not know, or they may bury their heads in the sand.
5. 2010 amendment: prohibited false imprisonment (e.g., when paparazzi say things to make the victims think they are not free to leave).
   (a) What if multiple paparazzi are involved?
6. First Amendment issues:[87]
   (a) Smolla: First Amendment should prohibit liability for intrusion in public places.
   (b) Chemerinsky: newsgathering should be subject to intermediate scrutiny. The CA Act would survive because it protects the privacy of the home.
   (c) Dienes: the Act "clearly target[s] the press." Because it imposes a disproportionate burden, it should be subject to strict scrutiny.

4.1.3 Video Voyeurism

1. What protections should people have from surveillance or intrusion in public places?

4.1.3.1 Video Voyeurism Prevention Act: 18 U.S.C. § 1801

1. Prevents intentionally capturing images of intimate areas under circumstances (1) where the person believed he could disrobe in privacy or (2) where intimate areas would not be visible to the public.[88]

4.2 Disclosure of Truthful Information

1. What types of disclosure should trigger civil liability?
2. How can liability for disclosure coexist with the First Amendment?

[87] Casebook pp. 104–06.
[88] Casebook pp. 107–108.

4.2.1 Public Disclosure of Private Facts

4.2.1.1 Restatement (Second) of Torts § 652(D): Publicity Given to Private Life

1. Liability exists when the matter publicized is (1) **highly offensive** and (2) **not of legitimate concern to the public**.
2. Seven states don't recognize the tort.[89]

4.2.1.2 Private Matters I—No Privacy for Events Occurring in Public: *Gill v. Hearst Publishing Co.*

"There can be no privacy in that which is already public."[90] Publishing to a wider audience doesn't matter (but the dissent disagrees).

1. Harper's published a photo of the plaintiffs in an affectionate pose at their public ice cream stand.
2. The court held that the plaintiffs voluntarily "waived their right of privacy so far as this particular public pose was assumed, for 'There can be no privacy in that which is already public.'"[91]
3. The photograph only "extended knowledge of the particular incident to a somewhat larger public than actually witnessed it at the time of occurrence."[92]
4. Justice Carter, dissenting:
   (a) The photo had no news value.
   (b) Consenting to public observation by a few does not mean consent to observation by millions of readers.[93]

4.2.1.3 Private Matters II—Involuntary Exposure: *Daily Times Democrat v. Graham*

Involuntary public exposure does not negate privacy protections.

1. The defendant published a photo of Graham as her dress was blown up when she exited a fun house.[94]
2. The newspaper argued that the photo was "a matter of legitimate news interest to the public . . . ."[95]

[89] Casebook p. 110.
[90] casebook p. 111.
[91] Casebook p. 111.
[92] Casebook p. 112.
[93] Casebook p. 112.
[94] Casebook p. 115.
[95] Casebook p. 115.

3. The court held that the photo was embarrassing and possibly obscene.

4. "To hold that one who is **involuntarily and instantaneously** enmeshed in an embarrassing pose forfeits her right of privacy merely because she happened at the moment to be part of a public scene would be illogical, wrong, and unjust."[96]

5. Commentary:

   (a) Courts vary in the privacy protections they give to information disclosed to small groups of people.[97] Lior Strahilevitz argues that protections should be based on how likely the information is to be disseminated beyond a particular group. For instance, someone can retain an interest in his HIV positive status even if 60 others (friends, family, doctors, support group members) knew about it. Three factors affect this likelihood: (1) how interesting the information is, (2) group norms, and (3) the structure of the group.[98]

   (b) Someone who gives comments to journalists can retract consent before publication.[99] Media entities can disseminate already public information, but further disclosure can lead to liability.[100]

4.2.1.4 Publicity—Special Relationship to the "Public": *Miller v. Motorola, Inc.*

What are the boundaries of "the public"? Can it be a small group? The court here held that "the public disclosure requirement may be satisfied by proof that the plaintiff has a special relationship with the 'public' to whom the information is disclosed," but many courts disagree.[101]

1. A nurse at Motorola disclosed that the plaintiff, an employee, had undergone mastectomy surgery.

2. Illinois law at the time required disclosure to be widespread and written.

3. The court here held that "the public disclosure requirement may be satisfied by proof that the plaintiff has a special relationship with the 'public' to whom the information is disclosed."[102]

4. (Many courts, and possibly the Restatement, disagree.[103])

5. Commentary:

[96] Casebook p. 116.
[97] Casebook p. 117–18.
[98] Casebook pp. 118–19.
[99] Casebook p. 119.
[100] Casebook p. 120.
[101] Casebook p. 121.
[102] Casebook p. 121.
[103] Casebook pp. 122–23.

(a) The widespread publicity requirement singles out broadcast media for restraints that don't apply to "gossip-mongers."[104]

(b) We often care more what a small group thinks of us.

4.2.1.5 Newsworthiness Test I: *Sipple v. Chronicle Publishing Co.*

There is no liability for disclosing facts that are (1) not private and (2) newsworthy.

1. Sipple thwarted an assassination attempt on President Ford. News stories reported that Sipple was prominent in the San Francisco gay community, outing Sipple to his family.[105]
2. Sipple sued for public disclosure of private facts.
3. The court here held (1) that the facts were not private ("hundreds of people in a variety of cities"[106] knew that Sipple was gay) and (2) the facts were newsworthy because they were "prompted by legitimate political considerations"[107] (e.g., did Ford fail to publicly thank Sipple because of bias against gays?).

4.2.1.6 What is newsworthy?

1. Courts use **three tests**:[108]
   (a) **Defer to editorial judgment** and make no distinction between news and entertainment.
   (b) Look to the **"customs and conventions of the community."**
   (c) Require a **"logical nexus"** between the person and the matter of legitimate public interest.
2. Volokh: we should eliminate the tort of public disclosure. (If he's right, is there anything that isn't relevant to fitness for office?)[109]
3. *Neff* (*Sports Illustrated* photo): "A factually accurate public disclosure is not tortious when connected with a newsworthy event even though offensive to ordinary sensibilities."[110]
   (a) Can this be reconciled with *Graham* (involuntary exposure at a fun house)? Maybe, on the basis that Graham's conduct was more voluntary, or on the basis that courts are more skeptical of protecting "involuntary" conduct while the plaintiff is intoxicated.

[104] Casebook p. 123.
[105] Casebook p. 123–24.
[106] Casebook p. 125.
[107] Casebook p. 126.
[108] Casebook p. 128.
[109] Casebook p. 129.
[110] Casebook p. 130.

4.

4.2.1.7 Newsworthiness Test II: *Shulman v. Group W Productions* The test for newsworthiness is "substantial relevance" to newsworthy subject matter. The court was deferential to editorial judgment.

1. Were Ruth's "appearance and words" of legitimate public concern?
2. Held: yes, it was newsworthy. The topic of public interest was the nurse's ability to handle the crisis.

4.2.1.8 Newsworthiness Test III: *Bonome v. Kaysen* The court applied the "logical nexus" test to protect the publication—even though it left behind significant human debris. Is anything fair game for a memoir?

1. Kaysen wrote a book that included scenes from her romantic relationship with Bonome—including scenes that attributed aggressive sexual force to him.
2. Held: the issue of public interest was the line between consent and non-consensual physical intimacy. There was a logical nexus between the material here and the issue of public interest.

4.2.2 First Amendment Limitations

4.2.2.1 Disseminating Public Records: *Cox Broadcasting Corp. v. Cohn* States can't prohibit the accurate publication of a name obtained from public records.

1. A reporter learned the name of a rape victim from an indictment available for public inspection. A news report published the victim's name. The victim's parents sued for invasion of privacy, citing a Georgia statute making it a misdemeanor to broadcast the name or identity of a rape victim.[111]
2. Public disclosure of private facts was the tort at issue.
3. The Court has avoided the question of whether laws can prevent publication of truthful but very private facts without violating the constitution.[112]
4. The Court here (Justice White) addressed a narrower question: can states prohibit the accurate publication of a name obtained from public records? Held, the State could not:[113]

[111] Casebook pp. 148–49.
[112] Casebook p. 150.
[113] Casebook pp. 150–51.

(a) Journalists serve a watchdog function. Allowing journalists to public the contents of public court records is important for government accountability and transparency.

(b) The state must have thought it was serving the public interest by putting the information in the public domain. The First and Fourteenth Amendments "command nothing less than that the States may not impose sanctions on the publication of truthful information contained in official court records open to public inspection."

(c) Another holding "would invite timidity and self-censorship."

4.2.2.2 Pseudonymous Litigation: *Florida Star v. B.J.F.*

1. "[I]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."[114]

4.2.2.3 *Bartnicki v. Vopper*

" . . . a stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a **matter of public concern** [but only for matters of public concern—not general conversations]."

1. Somebody received an anonymous tape of a conversation in which union negotiators threatened violence. The tape was recorded in violation of the Wiretap Act.[115]

2. Held: if the illegally obtained communication relates to a matter of public concern, the First Amendment prevents application of the Wiretap Act.

3. " . . . a stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern."

4. Justice Rehnquist, dissenting: this rule chills, rather than promotes, free speech.[116]

4.3 Dissemination of False or Misleading Information

4.3.1 Defamation

1. Defamation: **false information** that **harms the reputation** of the victim. Consists of libel (written) and slander (spoken).

[114] Casebook p. 155–60.
[115] Casebook p. 169 ff.
[116] Casebook p. 173 ff.

4.3.1.1 CDA § 230 and Broad Immunity for Service Providers: *Zeran v. AOL*

Computer service providers are not publishers (a category which includes distributors). Also, CDA § 230 did not create notice-based liability for service providers.

1. CDA § 230: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."
2. Somebody posted defamatory information about Zeran on an AOL message board.[117]
3. Is AOL a distributor? Traditionally, distributors are not liable unless they have *actual knowledge* of the defamatory statements.
4. The court rejected distributor liability. It held that computer service providers are not publishers (a category which includes distributors). It also held that CDA § 230 did not create notice-based liability for service providers.

4.3.1.2 *Blumenthal v. Drudge*

Does CDA § 230 provide too much immunity from tort liability?

1. Drudge wrote defamatory content about Blumenthal in his AOL column.[118] Blumenthal sued Drudge and AOL (here).
2. Held: even though AOL had editorial control, CDA § 230 granted it immunity from tort liability.

4.3.1.3 Public Officials and Actual Malice: *New York Times v. Sullivan*

To recover for defamation, public officials must prove **actual malice**—i.e., knowledge that the statement was **false or made with reckless disregard for whether it was false or not**.

1. A full-page *New York Times* ad criticized Sullivan's police department. Although he did not show pecuniary loss, the jury awarded $500,000 in damages for libel.
2. Justice Brennan:

[117] Casebook p. 185 ff.
[118] Casebook p. 188 ff.

(a) Can courts impose liability for libel against public officials in their public capacity without abridging constitutionally protected speech?[119]

(b) The speech here was constitutionally protected, but does it "forfeit[] that protection by the falsity of its statements . . . "?[120]

(c) Errors are inevitable in free debate. In order for that debate to have the "breathing space" it needs to survive, public officials can only recover if they prove that the defendant made the defamatory statements with **actual malice**—"with knowledge that it was false or with reckless disregard of whether it was false or not . . . . "[121]

3. Other Justices argued that defamation should be eliminated altogether for public officials, since the truth will emerge in the marketplace of ideas.[122]

4.3.1.4 Actual Malice and Private Citizens: *Gertz v. Robert Welch, Inc.*

Private citizens **do not** have to prove actual malice to recover for actual injuries. However, they have to prove actual malice to recover **punitive damages**, or else juries might punish unpopular views.

1. Gertz was the attorney representing a family whose son died from a police shooting. In a John Birch publication, Robert Welch, Inc. falsely accused Gertz of framing the officer as part of a communist conspiracy.[123]

2. Gertz sued for libel and won a $50,000 jury verdict. But the district court held that the *New York Times* actual malice standard should apply, and found for Welch.

3. Justice Powell:

   (a) Private individuals are more vulnerable to injury from defamation because they have **less access than public officials to channels of communication**. Thus, protections for them are greater.[124]

   (b) Public officials have **assumed the risk** of public life.

   (c) " . . . private individuals are not only more vulnerable to injury than public officials and public figures; they are also more deserving of recovery."[125]

   (d) Held: states can determine for themselves the standard of liability for defamation that injures private citizens.[126]

[119] Casebook p. 195.
[120] Casebook p. 196.
[121] Casebook p. 196.
[122] Casebook p. 197.
[123] Casebook p. 198.
[124] Casebook p. 199.
[125] Casebook p. 199.
[126] Casebook p. 200.

(e) However, punitive damages require a showing of actual malice. Otherwise, juries might "use their discretion to punish expressions of unpopular views."[127] Excessive jury discretion might also cause media self-censorship.

(f) Held: Gertz was not a public figure, so he did not have to prove actual malice.

4. Justice White, dissenting:

(a) The journalism industry is powerful and unlikely to be easily intimidated by the occasional defamation suit.[128]

4.3.1.5 Celebrity Divorces Are Not Public Controversies: *Time v. Firestone*

1. The court opinion in the Firestones' divorce described the couple's many "extramarital escapades."[129] *Time* published an article quoting the opinion, and Mary Firestone sued for libel.

2. Held: Firestone was not a public figure, even though she was extremely wealthy. "Dissolution of a marriage through judicial proceedings is not the sort of 'public controversy' referred to in *Gertz* . . . . "[130]

4.3.1.6 "Involuntary Limited-Purpose Public Figure": *Atlanta Journal-Constitution v. Jewell*

1. Jewell was the security guard who discovered a bomb at the Atlanta Olympics.

2. Held: by giving interviews, he became a "voluntary limited-purpose public figure" by injecting himself into a news story.

4.3.2 False Light

4.3.2.1 Overview

1. Liability if (1) **highly offensive** to a reasonable person and (2) the actor acted with knowledge or reckless disregard of the falsehood.[131] Different from defamation in that no harm to reputation is necessary.

[127] Casebook p. 200.
[128] Casebook p. 201.
[129] Casebook p. 202.
[130] Casebook p. 202.
[131] Casebook p. 205.

4.3.2.2 The First Amendment and False Light: *Time, Inc. v. Hill*

For matters of public concern, defendants are only liable for the false light tort if they acted with **knowledge of falsity or in reckless disregard for the truth**—i.e., actual malice. Courts are split on whether the actual malice standard also applies to private citizens (i.e., not public figures).

1. The Hill family was held hostage in their home for 19 hours. They were treated well, but a play about the event depicted violence and sexual abuse. *Life* published a story about the play which included re-enacted violent photos taken in the actual Hill home.[132]

2. The Hills claimed that the *Life* story gave the false impression that the play was accurate.

3. Held: the First Amendment precluded application of the false light statute to redress false reports of matters of public concern without proof that the defendant published the report with knowledge of its falsity or in reckless disregard for the truth.

4.3.3 Infliction of Emotional Distress

4.3.3.1 Overview

1. Liability arises when "**extreme and outrageous conduct intentionally or recklessly** causes severe emotional distress."[133]

4.3.3.2 IIED and Public Figures: *Hustler Magazine v. Falwell*

To claim intentional infliction of emotional distress from published material, public figures and officials must also show *New York Times* malice.

1. *Hustler* published parody of a Campari ad campaign featuring Jerry Falwell with the caption "Jerry Falwell talks about his first time" and other jabs. The ad included a disclaimer: "ad parody—not to be taken seriously."[134]

2. "...public figures as well as public officials will be subject to 'vehement, caustic, and sometimes unpleasantly sharp attacks."

3. Falwell and the appellate court take the view that if an outrageous utterance intended to cause emotional distress did in fact cause distress, "it is of no constitutional import whether the statement was a fact or an opinion, or whether it was true or false."

[132] Casebook p. 208.
[133] Casebook p. 211.
[134] Casebook p. 211 ff.

4. The Supreme Court, Justice Rehnquist: "We conclude that public figures and public officials may not recover for the tort of intentional infliction of emotional distress by reason of publications such as the one here at issue without showing in addition that the publication contains a false statement of fact which was made with 'actual malice,' i.e., with the knowledge that the statement was false or with reckless disregard as to whether or not it was true."

4.3.3.3 Special Protection: *Snyder v. Phelps*

There is special protection for public speech on matters of public concern.

1. Members of the Westboro Baptist Church protested viciously at a military funeral.[135]
2. Justice Roberts: the speech receives "special protection" because it was "at a public place on a matter of public concern . . . ."[136]

4.4 Appropriation of Name or Likeness

4.4.1 Introduction

1. Appropriation: privacy-based; concerned with dignity.
2. Right of publicity: property-based; concerned with commercial reward.[137]

4.4.2 Name or Likeness: *Carson v. Here's Johnny Portable Toilets, Inc.*

Appropriation of identity can occur without using a name or likeness—e.g., a catchphrase like "Here's Johnny!"

1. Carson brought two actions, based on the right to privacy and the right to publicity.
2. Right to privacy: this tort is based on embarrassment, but there is no evidence here that Carson was embarrassed.[138]
3. Right to publicity: the "name or likeness" standard is too low. Since the phrase "Here's Johnny" is so closely associated with Carson, the court found an appropriation of his identity.[139]

[135] Casebook p. 214 ff.
[136] Casebook p. 216.
[137] Casebook p. 221.
[138] Casebook p. 233.
[139] Casebook p. 234.

4. Judge Kennedy, dissenting: the court's holding allows celebrities to remove phrases from the public domain forever.

5. Courts have subsequently extended the "name or likeness" standard much further.[140]

4.4.3 For One's Own Use or Benefit: *Raymen v. United Senior Association, Inc.*

The tort of appropriation does not apply to noncommercial use. The exception applies to news (*Finger v. Omni*, below), parody, satire, etc. (e.g., the Beach Boys song "Johnny Carson").

1. USA, Inc. used a photo of Raymen kissing his partner to promote its anti-AARP advocacy.

2. The court held that USA used the photo to "discuss[] policy issues," rather than to gain commercial advantage. Since its use was noncommercial, Raymen could not recover for appropriation.[141]

4.4.4 Connection to Matters of Public Interest: *Finger v. Omni Publications International, Ltd.*

News media can use a person's name or likeness without incurring liability as long as there is a "real relationship" between the person and the story. (But what about the fact that most news organizations are also commercial entities?)

1. The appropriation tort does not protect against the use of one's name or likeness for news, art, etc.—i.e., uses that are not purely commercial.[142]

2. In New York, the right of the media to use someone's name or likeness depends on a **"real relationship"** between the use and the article. It can't be an "advertisement in disguise."[143]

3. Omni published a photo of the Fingers and their six kids alongside an article about the effect of caffeine on in-vitro fertilization. The court held (tenuously) that the subject of the article was fertility in general; thus, there was a real connection between the photograph and the article.[144]

4.4.5 Right of Publicity and First Amendment Limitations: *Zacchini v. Scripps-Howard Broadcasting Co.*

---

[140] Casebook pp. 225–27.
[141] Casebook p. 231.
[142] Casebook p. 233.
[143] Casebook p. 234.
[144] Casebook pp. 235–36.

Letting a news broadcast show an entire act threatens the economic value of the performance. The First Amendment doesn't allow news organizations to undermine performers' publicity rights.

1. A local TV station broadcast the entirety of Zacchini's human cannonball act without his consent.
2. The Ohio Supreme Court held that the First Amendment protected the broadcast. The Supreme Court granted cert to decide whether the First Amendment immunized the broadcaster from liability under the appropriation tort.[145]
3. The Court drew two distinctions between the appropriation tort, at issue here, and the false light tort (at issue in *Time, Inc. v. Hill*):[146]
   (a) False light is concerned with reputation, while appropriation is concerned with a proprietary interest.
   (b) Second, false light attempts to minimize publication, while appropriation decides who gets to do the publishing.
4. Held: the First and Fourteenth Amendments do not immunize the broadcaster from needing to pay the performer for broadcasting the entire act.[147]

4.4.6 Imitators: *Estate of Presley v. Russen*

Imitators are liable under the appropriation tort if they don't add substantial value.

1. Russen ran a show that imitated Elvis's style. Elvis's estate sued for infringement of the right of publicity.
2. Held: the imitation show "serves primarily to commercially exploit" Elvis's likeness without adding anything of value.[148]
3. However, the court did not grant a preliminary injunction because the plaintiffs could not show that continued performances would cause "immediate, irreparable harm to the commercial value of the right of publicity . . . ."[149]

[145] Casebook p. 239.
[146] Casebook p. 240.
[147] Casebook p. 240.
[148] Casebook p. 242.
[149] Casebook p. 244.

§ 5 Privacy and Law Enforcement

5.1 The Fourth Amendment and Emerging Technology

5.1.1 Introduction

1. *Ex parte Jackson*: Fourth Amendment does not protect the outside of letters.[150]

2. **Special needs doctrine**: schools, government workplaces, and certain highly regulated business.[151]

3. Sobriety checks: ok, because they aim to protect road safety. Drug violation checks: not ok, because aim to detect general criminal wrongdoing.[152]

4. *Terry* stops: upon reasonable suspicion.[153]

5.1.2 Wiretapping, Bugging, and Beyond

5.1.2.1 Phone Wiretapping: *Olmstead v. United States*

Early in the 20th Century, the Court read the Fourth Amendment narrowly to exclude protections for phone wiretapping.

1. The government tapped the phones of suspected bootleggers. The issue was whether the wiretapping violated the Fourth and Fifth Amendments. The Court (Taft, J.) held that there had been no search or seizure, distinguishing electronic wiretapping from postal searches.

2. "The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The [Fourth] amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the used of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."

3. Justice Brandeis, dissenting:

   (a) "The mail is a public service furnished by the government. The telephone is a public service furnished by its authority. There is, in essence, no difference between the sealed letter and the private telephone message."

[150] Casebook p. 249.
[151] Casebook p. 252.
[152] Casebook p. 252–53.
[153] Casebook p. 254.

5.1.2.2 Secret Recordings of In-Person Conversations: *Lopez v. United States*

The Court adopted the **risk theory**: if you break the law, you run the risk that the offer "will be accurately reproduced in court by . . . mechanical rendering."

1. No eavesdropping here.[154]
2. The device was not planted through unlawful physical invasion.

5.1.2.3 REOP Test: *Katz v. United States*

A search occurs when the government violates a person's reasonable expectation of privacy.

1. Katz made a phone call about gambling in a telephone booth, which the government listened to without entering the booth. The Court held that it was a search.
2. Justice Stewart:
   (a) "In the first place, the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.' Secondly, the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"
   (b) " . . . the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."
3. Justice Harlan: " . . . there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"

5.1.2.4 Undercover Agent: *United States v. White*

1. "Inescapably, one contemplating illegal activities must realize the risk that his companions may be reporting to the police."
2. Justice Harlan, dissenting: third-party bugging will undermine trust and confidence. A warrant should be required.

[154] Casebook p. 263.

5.1.3 The Reasonable Expectation of Privacy Test and Emerging Technology

5.1.3.1 Third Party Doctrine: *Smith v. Maryland*

A person does not have a reasonable expectation of privacy in information that he voluntarily discloses to third parties.

1. A phone company's installation of a pen register does not constitute a search under the Fourth Amendment. Applying the Katz test, the Court held that Katz had no legitimate expectation of privacy in the numbers he dialed. He "assumed the risk that the company would reveal the information to the police . . . ."
2. Justice Marshall, dissenting: "In my view, whether privacy expectations are legitimate within the meaning of Katz depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society."

5.1.3.2 Canine Sniff: *United States v. Place*

1. Canine sniffs are sui generis. " . . . exposure of defendant's luggage, which was located in a public place, to a trained canine . . . did not constitute a 'search' within the meaning of the Fourth Amendment . . . ."[155]

5.1.3.3 Dog Sniff II: *Illinois v. Caballes*

1. A dog detected marijuana in the trunk during a traffic stop.
2. Held: government conduct that only reveals the presence of contraband compromises no legitimate privacy interest.
3. Justice Souter, dissenting: dogs are fallible, and they are used to gather information about private spaces.
4. Justice Ginsburg, dissenting: use of a drug detection dog changes the nature of a traffic stop.

5.1.3.4 Are Dogs Fallible? *Florida v. Harris*

1. If dogs are often wrong, does that preclude probable cause?
2. Dogs' certification and training are adequate indications of their reliability. (Unanimously held.)

[155] Casebook p. 285.

5.1.3.5 Dogs and Curtilage: *Florida v. Jardines*

1. Majority (Justice Scalia): a dog sniff on the front porch of a home is a search because it's a trespass.

2. The front porch is a "classic exemplar" of **curtilage** (the protected area around a house), and dog sniffs are an unlicensed physical intrusion.

5.1.3.6 Trash Bags: *California v. Greenwood*

1. Police searched trash bags that Greenwood left out for collection.[156]

2. Held: no reasonable expectation of privacy in trash bags left on the street.

5.1.3.7 Plain View, Open Fields, and Curtilage

1. **Plain view doctrine**: no expectation of privacy in things that can be seen from a public vantage point.[157]

2. **Open fields doctrine**: no expectation of privacy in the open fields a person owns—but curtilage is an exception.

5.1.3.8 Aerial Surveillance: *Florida v. Riley*

1. Officers inspected a backyard from a helicopter at 400 feet.

2. Held: no REOP. No intimate details were revealed and there was no disturbance.

5.1.3.9 Industrial Curtilage: *Dow Chemical v. United States*

1. There is no "industrial curtilage." Taking photographs of an industrial plant from navigable airspace does not violate the Fourth Amendment.[158]

5.1.3.10 Thermal Imagiging: *Kyllo v. United States*

1. The government used thermal imaging to detect Kyllo's marijuana growing operation inside his home.[159]

2. Justice Scalia: "Where, as here, the government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment 'search,' and is presumptively unreasonable without a warrant."

[156] Casebook p. 290.
[157] Casebook p. 293.
[158] Casebook p. 303.
[159] Casebook p. 306.

3. The core of the Fourth Amendment is the "right of a man to retreat into his own home and there be free from unreasonable government intrusion."

4. Justice Stevens: this case did not involve "intimate details" of the home. Rather, it involved "indirect deductions from 'off-the-wall' surveillance" of amorphous blobs.

5.2 Federal Electronic Surveillance Law

5.2.1 Section 605 of the Federal Communications Act

1. Federal Communications Act, 1934: prevented unauthorized interception or divulgence of communications.[160]

2. Did not apply to state prosecutions or bugging (i.e., non-wire communications).

5.2.2 Title III

1. Enacted in 1968 in response to *Katz*; amended in 1986 as the Wiretap Act.

2. Prevented all warrantless federal, state, and private wiretapping, but allowed one-party consent.[161]

3. Excluded wiretaps for national security purposes.

5.2.3 The Electronic Communications Privacy Act

1. See Schwartz and Solove, "ECPA in a Nutshell."

2. Amended Title III (with the Wiretap Act) and added two new acts (SCA and the Pen Register Act).

3. Types of communications:[162]

   (a) **Wire communications**: travel through a wire or similar medium. Must include a human voice.

   (b) **Oral communications**: typically intercepted through bugs.

   (c) **Electronic communications**: all non-wire, non-oral communications—e.g., email.

4. Statutory structure:

   (a) Wiretap Act.[163]

[160] Casebook p. 313.
[161] Casebook p. 315.
[162] Casebook p. 316.
[163] Casebook p. 317–19.

   (b) Stored Communications Act.[164]
   (c) Pen Register Act.[165]

5. **Video**: if it's oral, it's covered by the Wiretap Act. If it's just silent video, federal electronic surveillance law does not apply.[166]

6. Electronic surveillance orders under wiretap law have recently expanded.[167]

7. State electronic surveillance law: many require consent of all parties to a conversation.

8. Websites are only sometimes ECS providers. Normal retail sites, e.g. L.L. Bean, are not ECS providers.

5.2.4 The Communications Assistance for Law Enforcement Act

1. Telecom providers must assist legally authorized surveillance.

2. Networks must be designed to telecoms can intercept communications and provide them to law enforcement.

3. VoIP qualifies.

5.3 Digital Searches and Seizures

5.3.1 Searching the Contents of Computers: *United States v. Andrus*

Third parties have apparent authority to consent to a search when an officer reasonably but erroneously thinks the third-party has authority to consent.

1. Is the consent of the father of the suspect valid to search the computer, even if the father didn't know the password? The officers used forensic tools to let them circumvent the password protection.[168]

2. Valid third-party consent can arise through the third party's actual or apparent authority. The third party has apparent authority even when the officer erroneously thinks the third party has authority to consent.

3. Passwords on a computer are analogous to locks.

4. Officers reasonably believed the father had authority to consent.

[164] Casebook p. 319–321.
[165] Casebook p. 322.
[166] Casebook p. 322.
[167] Casebook p. 323 ff.
[168] Casebook p. 336 ff.

5.3.2 Email—Interception vs. Storage: *Steve Jackson Games v. United States Secret Service*

The Wiretap Act's protection against "interception" does not apply to stored electronic communications. "Electronic communication" under the Wiretap Act does not include stored data (so the SCA applies).

1. SJG operated a bulletin board that allowed users to exchange private messages ("E-mail"). The Secret Service obtained a warrant to search the servers for evidence of computer crimes. It seized 162 unread, private messages.[169]
2. Plaintiffs sued for violation of the Wiretap Act (18 U.S.C. § 2510–21) and the Stored Communications Act (§ 2701–11).
3. Is seizure of sent but unread messages an "intercept" under § 2511(1)(a)[170]?
   (a) No. "'Electronic communication" does not include electronic storage of such communications."[171]
4. However, the Secret Service is liable under the SCA.[172]

5.3.3 Kerr, "The Problem of Perspective in Internet Law"

1. Does the Fourth Amendment protect stored emails?[173]
2. *Internal perspective*: the Internet is a virtual world. Email is analogous to postal mail, so a warrant is required.
3. *External perspective*: the message passes through a third party. No warrant is required to get email stored with a third party.

5.3.4 Privacy Expectations in Email Contents: *United States v. Warshak*

There is a Fourth Amendment reasonable expectation of privacy in the contents of emails. The SCA is unconstitutional to the extent that it lets government compel ISPs to turn over email contents without a warrant. (No other circuit has weighed in.)

1. Warshak was indicted for several crimes related to his pharmaceutical business. Law enforcement seized 27,000 of his emails from his ISP without a warrant.

[169] Casebook pp. 345–46.
[170] Anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."
[171] Casebook pp. 346–47.
[172] § 2701(a): "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility."
[173] Casebook pp. 348–49.

2. Emails are private, just like letters.[174]
3. *Miller* (bank records) do not control because (1) these emails were confidential communications, not business records and (2) the ISP was an intermediary, not the intended recipient.[175]
4. The SCA is unconstitutional to the extent that it lets government compel ISPs to turn over email contents without a warrant.[176]
5. But the evidence should not be suppressed because the officers relied in good faith on the SCA.
6. Held: "the government *did* violate Warshak's Fourth Amendment rights by compelling is Internet Service Provider ('ISP') to turn over the contents of his emails. However, we agree that agents relied on the SCA in good faith, and therefore hold that reversal is unwarranted."[177]

5.3.5 REOP in ISP Records: *United States v. Hambrick*

Subscribers do not have a REOP in the subscription data they give to their ISPs. Moreover, there is no exclusionary rule in the SCA—only damages provisions.

1. An undercover detective subpoenaed an ISP to get subscriber data for someone posting criminal messages in a chat room. The subpoena was invalid, but the government still obtained the data.
2. The defendant argued that ECPA creates a Fourth Amendment REOP in subscriber data. The court disagreed.[178]
3. There is no exclusionary rule in the SCA; civil damages are the only remedy.

5.3.6 Suppression: *McVeigh v. Cohen*

Suppression is warranted if the government breaks the law to get information from a service provider.

1. The Navy used social engineering to get information from AOL to investigate a don't ask, don't tell issue. McVeigh didn't "tell," but the Navy launched a "search and 'outing' mission" against him.

[174] Casebook p. 352–53.
[175] Casebook p. 354–55.
[176] Casebook p. 355.
[177] Casebook p. 352.
[178] Casebook pp. 358–59.

2. Held: the government violated ECPA by failing to obtain a subpoena. Moreover, it solicited AOL to break the law, since 18 U.S.C. § 2703(c)(1)(B) puts the burden on the service provider to withhold information from the government.[179]

5.3.7 No Suppression for IP Addresses and URLs: *U.S. v. Forrester*

1. The use of a pen register is not a Fourth Amendment search.[180]
2. The collection of Internet metadata here was constitutionally indistinguishable from pen register collection. The Pen Register Act does not provide for suppression, so there was no suppression here.

5.3.8 Keylogging: *United States v. Scarfo*

1. Agents installed a physical keylogger.
2. The keylogger was only activated when the modem was turned off, so it did not "intercept" a wire communication.

5.4 National Security and Foreign Intelligence

5.4.1 Warrants for Domestic Surveillance: *United States v. United States District Court* (the *Keith* case)

1. Three categories of domestic security activity:
   (a) Criminal investigations.
   (b) Domestic security investigations.
   (c) Foreign security investigations.
2. Domestic surveillance for national security risks infringing "privacy of speech," so a warrant is required.[181]
3. Foreign surveillance for national security purposes may be different.[182]

5.4.2 Foreign Intelligence Surveillance Act (FISA)

5.4.2.1 Overview

1. FISA applies when foreign intelligence gathering is a "significant purpose" of the investigation. (Otherwise, ECPA applies.)[183]
2. **National Security Letters**: the FBI can use them to get information from third parties, including under the Pen Register Act and SCA (but not the wiretap act). Includes a gag order provision.

[179] Casebook p. 363.
[180] Casebook p. 366 ff.
[181] Casebook p. 380.
[182] Casebook p. 381.
[183] Casebook p. 385–86.

5.4.2.2 Emergency Exception to FISA: *Global Relief Foundation, Inc. v. O'Neil*

1. The emergency FISA exception allows warrantless searches.[184]

5.4.2.3 The Wall: *United States v. Isa*

1. FISA authorizes retention of evidence that is "evidence of a crime." The crime need not be related to foreign intelligence—as long as foreign intelligence gathering was "a significant purpose" of the investigation.

5.4.2.4 Foreign Intelligence as Criminal Evidence: *In re Sealed Case*

1. As long as a "significant purpose" of the investigation is gathering foreign intelligence, the evidence acquired can be used in a criminal case.[185]

5.4.3 NSA Surveillance Program

5.4.3.1 11/30/11 FISC Order, Judge Bates

1. The FISC is satisfied that the government has fixed the defects in its minimization procedures that the court had previously identified.

5.4.3.2 8/29/13 FISC Order, Judge Eagan

1. The government's bulk collection of telephony metadata is consistent with § 215 of the USA PATRIOT Act and the Fourth Amendment.

5.4.4 *Clapper v. Amnesty International*

Plaintiffs lacked standing to challenge the FISA Amendments Act of 2008 (FAA).

1. Several groups sued the government over the FAA, which authorizes the surveillance of non-U.S. persons outside the U.S.
2. Justice Alito:
   (a) Respondents do not have standing because:
      i. The injury must be concrete, particularized, and actual or imminent.
      ii. The harm here was overly speculative.
      iii. Expenditures in response to hypothetical harm (e.g., traveling abroad to avoid having communications monitored) do not "manufacture standing."[186]

[184] Casebook p. 388.
[185] Casebook p. 397.
[186] 2.

iv. The alleged injuries here are different than other standing cases on which the respondents rely.[187]

3. Justice Breyer, dissenting:

   (a) The question was whether the injury was "actual or imminent."[188]

   (b) There is a high likelihood that under § 1881(a) the government will intercept some of the plaintiffs' communications.[189] The harm is not "speculative."[190]

[187] 3.
[188] 2.
[189] 6, 9.
[190] 10.

§ 6 Health Privacy

6.1 Confidentiality of Medical Information

6.1.1 HIPAA

1. HIPAA: 1996. HHS regulations implementing HIPAA: November 1999. Primarily about **portability**.[191]

2. **Privacy rule** (2000): final version of HIPAA regulations.[192] Became effective in 2003. Covers the use of protected health information—see casebook pp. 465–68.

3. **Security rule**: published 2003, effective 2005. Covers the security of electronic personal health information. See casebook pp. 468–69.

4. Criminal enforcement—see casebook pp. 471–73.

5. Law enforcement access and the third party doctrine–see casebook pp. 473–75. The New York Court of Appeals denied a law enforcement subpoena for health records, despite the fact that HIPAA (§ 164.512(f)) allowed it.[193]

6. **Covered entities**: health plans, clearinghouses, providers.

7. **Marketing**: authorization is required, but not for the plan's own services and products.

8. Covered entities must make **minimum necessary use and disclosures**.

9. May disclose to a **business associate** if there are assurances of safeguards.

10. CEs must implement three kinds of **safeguards**: administrative, physical, and technical.

6.1.2 HITECH Act

1. Facilitates electronic health records. Increases penalties and expands security rule to business associates.

2. New data breach notification requirements if information has been "compromised." Breach notifications are necessary in all situations except those in which the CE or BA shows a low probability that the information has been compromised.

[191] Casebook p. 463 ff.
[192] Casebook p. 463.
[193] Casebook p. 475.

6.2 Constitutional Protection of Medical Information

6.2.1 Two Privacy Interests: *Whalen v. Roe*

There are two types of privacy interests: **informational** and **decisional**.

1. New York kept records of Schedule II drug prescriptions.
2. Plaintiffs argued that the records would make people decline treatment out of fear that the records would be misused.
3. **Two kinds of privacy interests**:[194]
   (a) **Informational**: avoiding disclosure of personal matters.
   (b) **Decisional**: independence in making important decisions.
4. The NY statute does not threaten either enough to establish a constitutional violation.

6.2.2 42 U.S.C. § 1983 and "Constitutional Torts"

1. Provides civil remedies for constitutional violations. Constitutional violations become tort actions, enabling plaintiffs to win damages and injunctive relief.[195]
2. There must be a **state actor**. Plaintiffs *cannot* directly sue states because of the Eleventh Amendment, but they *can* sue any state or local government official. They can also sue local governments when their policy or custom inflicts the injury.

6.2.3 Limited Access to Patient Records: *Carter v. Broadlawns Medical Center*

1. BMC had a policy of allowing its chaplain open access to medical records.
2. Plaintiffs alleged the policy violated patients' confidentiality.
3. Held: the chaplain could not have open access, but he could know about the patient's "basic problem" (e.g., a suicide attempt).

6.2.4 Government Disclosure of HIV Status: *Doe v. Borough of Barrington*

1. Police officers revealed to the defendant's neighbors the fact that he was HIV positive.[196]

[194] Casebook p. 505.
[195] Casebook p. 510–11.
[196] Casebook p. 513.

2. Held: the Constitution prevents government disclosure of HIV status.[197] To disclose a person's HIV status, the state must show a compelling government interest that outweighs the substantial privacy interest.[198]

6.2.5 *Doe v. Southeastern Pennsylvania Transportation Authority*

The seven *Westinhouse* factors weight the privacy interest against competing interests.

1. As part of a health insurance plan review involving auditing of prescription drug records, the defendant's employer learned of the defendant's HIV-positive status. He alleges he was treated differently at work after the disclosure.[199]

2. Each disclosure to a new person was a separate disclosure. However, disclosures to the company doctors were not actionable because they already knew of the defendant's status.[200]

3. *Westinghouse*: seven factors to weight the privacy interest against competing interests.

4. Held: the intrusion here was minimal. On balance, the employer's interests are more substantial–e.g., containing healthcare costs.[201]

6.3 Genetic Information

6.3.1 Overview

1. Background on DNA—see casebook pp. 526–27.

2. At least 18 state genetic privacy statutes.[202]

3. DNA can be a **"future diary."**[203]

4. Issues in DNA databases—see casebook pp. 553–59.

6.3.2 Taking DNA Samples from Arrestees: *Maryland v. King*

Swabbing the cheek of an arrestee to get a DNA sample is reasonable under the Fourth Amendment.

[197] Casebook p. 514.
[198] Casebook p. 515.
[199] Casebook pp. 516–18.
[200] Casebook p. 519.
[201] Casebook p. 521.
[202] Casebook p. 538.
[203] Casebook p. 539.

1. Officers took a cheek swab after arresting King on assault charges. His DNA matched samples from an unsolved rape eight years earlier. He was convicted of the rape.[204]

2. Is it reasonable under the Fourth Amendment to take a cheek swabbing for DNA samples of arrestees?

3. Justice Kennedy:

   (a) DNA testing is highly useful for law enforcement.

   (b) The intrusion of a cheek swab is negligible. Legitimate government interests outweigh this minimal intrusion.

   (c) The government has several interests in using DNA samples:

      i. Identifying who is being arrested.

      ii. Other reasons—see syllabus p. 3.

   (d) The defendant's privacy interests do not outweigh the government's interests. The intrusion is minimal, the sampling does not reveal genetic traits, and it is unlikely to reveal medical information.

4. Justice Scalia:

   (a) In this case, identification of the suspect cannot possibly be the purpose of taking the DNA sample. (No difference between DNA sampling and fingerprinting.)

[204] See slip opinion.

§ 7 Privacy and Government Records and Databases

7.1 Public Access to Government Records

7.1.1 Public Records and Court Records

1. Court records are public in all states.[205]

7.1.1.1 Pseudonymous Civil Litigation: *Doe v. Shakur* In civil suits, plaintiffs sometimes cannot remain anonymous. However, judges have discretion.

1. Can a victim of sexual assault bring civil charges under a pseudonym?[206]
2. Does the plaintiff's privacy right outweigh judicial openness?
3. Held: in a civil context, the victim does not have a right to use a pseudonym.

7.1.2 The Freedom of Information Act

1. Transparency of federal documents is the default.
2. Nine exemptions: casebook pp. 642–43.
3. Two privacy exemptions.[207] There's a higher threshold for law enforcement files.

7.1.2.1 Rap Sheets: *DOJ v. Reporters Committee for Freedom of the Press* FOIA does not compel disclosure of rap sheets. They have "practical obscurity" and reveal little about "what the government is up to."

1. Much rap sheet information is public, but not in the complete form that the DOJ maintains—hence the "practical obscurity of rap sheets."
2. There's a high interest in maintaining practical obscurity. Moreover, personal rap sheets have little to do with "what the government is up to."
3. Held: FOIA does not compel disclosure of rap sheets.

7.1.2.2 Family Privacy vs. Government Misconduct: *NARA v. Favish* Disclosure outweighs privacy interests only when there is reasonable evidence of government impropriety.

1. Allan Favish sought disclosure from NARA of death-scene photographs of Vincent Foster, Jr., deputy counsel to President Clinton, whose death was ruled a suicide.

[205] Casebook p. 636.
[206] Casebook p. 637 ff.
[207] Casebook p. 643.

2. Held: none of the photos can be released because (1) exemption 7(C) is broad enough to protect a family's privacy interest in restricting photos of a deceased relative, and (2) the family's privacy interest outweighs the public interest.

3. "Only when the FOIA requester has produced **evidence sufficient to warrant a belief by a reasonable person that the alleged Government impropriety might have occurred** will there be a counterweight on the FOIA scale for a court to balance against the cognizable privacy interests in the requested documents."

7.1.3 Constitutional Limitations on Public Access

7.1.3.1 Arrest Records: *Paul v. Davis*

1. States can publish arrest records.[208]

7.1.3.2 Privacy in Criminal Records: *Cline v. Rogers*

1. "... there is no constitutional right to privacy in one's criminal record."[209]

7.1.3.3 Police Records after Whalen: *Scheetz v. The Morning Call, Inc.*

1. After *Whalen*, information in police records is not private.[210]

7.1.3.4 Megan's Laws: *Paul P. v. Verniero*

1. Megan's Laws require public disclosure of sex offender locations.

2. Here, the plaintiff challenged the constitutionality of the NJ Megan's Law.

3. Held: "Megan's Law does not restrict plaintiffs' freedom of action with respect to their families."[211]

7.2 Government Records of Personal Information

7.2.1 Fair Information Practices

1. FIPs are the rights and responsibilities associated with the transfer and use of personal information. Typically, they assign rights to individuals and responsibilities to organizations.[212]

[208] Casebook p. 678.
[209] Casebook p. 681.
[210] Casebook p. 682–84.
[211] Casebook p. 690.
[212] Casebook p. 699.

7.2.2 The Privacy Act (1974)

1. Enacts FIPs into federal law.[213]
2. Regulates how federal agencies collect and use personal information.
3. Creates a private right of action.

7.2.2.1 Hunting Records: *Quinn v. Stone*

1. Hunting rosters are public records under the Privacy Act.
2. Held: plaintiffs could show an adverse effect from revelation of information on hunting records and time cards.

7.2.2.2 Actual Damages: *Doe v. Chao*

1. Under the Privacy Act, plaintiffs must prove some actual damages in order to qualify for the minimum statutory award of $1,000.

7.2.3 The Driver's Privacy Protection Act

1. State DMVs can disclose personal information only with opt-in (with some exceptions).[214]

[213] Casebook p. 701.
[214] Casebook p. 754.

§ 8 Privacy of Financial and Commercial Data

8.1 The Financial Services Industry and Personal Data

8.1.1 Fair Credit Reporting Act

1. 1970: FCRA.[215]

2. Scope turns on the definition of "consumer report." Most reports dealing with consumer credit fall within this definition.[216]

3. Statutory requirements: see casebook pp. 758–65.

8.1.1.1 Legitimate Business Need: *Smith v. Bob Smith Chevrolet, Inc.* FCRA does not allow the use of credit reports beyond "legitimate business needs," narrowly construed.

1. Smith agreed to buy a car from Bob Smith. Part of the deal involved a trade-in of his existing car, for which Bob Smith would assume the remainder of unpaid loans. He also got a GM employee discount.[217]

2. After the sale, Bob Smith learned that it had mistakenly doubled Smith's discount. It accessed Smith's consumer report. Smith argued that Bob Smith negligently and willfully violated FCRA.[218]

3. First, Bob Smith argued that it accessed the report as part of a "business transaction." The court held that Congress intended to allow access to reports in this context for the purpose of determining the customer's eligibility for a benefit. But in this case, the use was not in connection with a standard business transaction. It was not for a reason beneficial to the consumer. Smith, the buyer, did not initiate the transaction under which Bob Smith accessed his consumer report.[219]

4. Second, Bob Smith argued that it accessed the report in connection with "collection of an account of the consumer." But a debt did not actually exist here. Bob Smith *alleged* a debt but did not prove its existence.[220]

5. Whether Bob Smith's noncompliance was willful was a jury question.[221]

[215] Casebook p. 757 ff.
[216] Casebook p. 758.
[217] Casebook p. 765–77.
[218] Casebook p. 766.
[219] Casebook p. 767-68.
[220] Casebook p. 768–69..
[221] Casebook p. 769.

8.1.1.2 Liability for Inaccurate Credit Reports: *Sarver v. Experian Information Solutions*

1. Experian inaccurately reported information on Sarver's credit report.[222]
2. Held: credit reporting agencies are not liable if they take "reasonable procedures to assure maximum possible accuracy." Liability requires notice of systemic problems or individual defects.

8.1.2 The Use and Disclosure of Financial Information

8.1.2.1 The Graham-Leach-Bliley Act

1. Protects only **nonpublic personal information** (NPPI)[223]—e.g., first and last name plus any of the following: SSN, driver's license number, credit card number, etc.
2. Authorizes sharing between **affiliated companies**. Customers must be told about the sharing, but they can't prevent it. ("Affiliated" means it controls, is controlled by, or is under common control with the other.)
3. Also authorizes sharing with **unaffiliated companies**, but customers must be able to opt out.
4. Requires an annual privacy notice.
5. FTC and other agencies are to establish privacy and security regulations for regulated entities.

8.1.2.2 State Financial Regulation

1. See casebook pp. 783–85.

8.1.3 Identity Theft

8.1.3.1 Identity Theft Statutes

1. Identity Theft Assumption and Deterrence Act: federal, 1998.[224]
2. FCRA/FACTA—see below.
3. More than 40 state laws.
4. Solove: the credit system enables identity theft, e.g., by the frequent use of SSNs as identifiers.[225]

[222] Casebook p. 772.
[223] Casebook p. 780 ff.
[224] Casebook p. 786.
[225] Casebook p. 787–88.

8.1.3.2 Tort Law: *Wolfe v. MBNA America Bank*

Identity theft is foreseeable and preventable, so banks have to implement reasonable and cost-effective means to address it.

1. Wolfe sued MBNA after his identity was stolen. MBNA moved to dismiss.
2. MBNA had issued a credit card in Wolfe's name to the thief. Wolfe argued that MBNA had a duty to identify "the accuracy and authenticity" of the credit application.[226]
3. MBNA relied on a South Carolina decision holding that banks are not negligent if they issue credit cards on the basis of fraudulent applications.[227]
4. The court here held that the South Carolina decision was flawed because it was foreseeable that injury would result from negligent issuance of a credit card. Banks must take reasonable measures to prevent identity theft.[228]

8.1.3.3 FCRA and Emotional Damages: *Sloane v. Equifax*

1. An identity thief ruined Sloane's credit.[229]
2. FCRA provides a private right of action.
3. Sloane sought damages for emotional distress.
4. Held: defamation law offers guidance. Here, there was almost no harm to Sloane's reputation. However, the court sustained damages of $150,000 (less than the $245,000 than the jury awarded, but still significant).

8.2 Commercial Entities and Personal Data

8.2.1 Governance by Tort

8.2.1.1 Intrusion upon Seclusion and Appropriation: *Dwyer v. American Express Co.*

Selling cardholder data is not actionable as intrusion upon seclusion or appropriation.

1. In a class action, American Express cardholders sued over the company's practice of selling cardholder data.[230]
2. Intrusion upon seclusion:

[226] Casebook p. 789.
[227] Casebook p. 790.
[228] Casebook p. 791.
[229] Casebook p. 792.
[230] Casebook p. 799.

(a) Elements:

i. Unauthorized intrustion.
ii. Offensive or objectionable.
iii. Private matter.
iv. Anguish and suffering.

(b) Held: plaintiffs failed to satisfy the first element because they voluntarily disclosed the information to AMEX. Names and addresses are disclosed (for lists of consumers with specific spending habits), but no financial information is disclosed.[231]

(c) Appropriation:

i. Elements: appropriation of name or likeness without without consent for another's benefit.
ii. Held: individual cardholder names do not create value for the defendants; moreover, disclosure or sale does not deprive cardholders of any value.[232]

3. Is there harm in knowing patterns of consumption? See pp. 802–04.

8.2.1.2 Duty of Care for Private Investigators: *Remsberg v. Docusearch, Inc.* The risk of criminal misconduct due to stalking and ID theft are sufficiently foreseeable to create a duty on the investigator to exercise reasonable care in disclosing a third person's information to a client.

1. Youens hired Docusearch to get Boyer's personal information. Docusearch lied to get some of the information. Youens later found and killed Boyer.[233]

2. Private citizens generally have no duty to protect others from the criminal acts of third parties.[234] However, people have a duty not to create risks of foreseeable harm. So, if a private investigator's disclosure of information creates a foreseeable risk of criminal misconduct, the investigator owes a duty of care.

3. Stalking and identity theft are foreseeable.[235]

4. Intrusion upon seclusion:

(a) Somebody might have an action against a third party who obtained that person's SSN from a credit reporting agency, but that person must prove that the intrusion would have been offensive to a reasonable person.

[231] Casebook p. 800.
[232] Casebook p. 801.
[233] Casebook p. 804.
[234] Casebook p. 805.
[235] Casebook p. 806.

(b) What about obtaining a work address through a pretextual phone call? If the address is readily available to the public, it's not private and so there cannot be an action for intrusion upon seclusion.

5. Appropriation:

   (a) Not actionable if used for a purpose other than taking advantage of the person's reputation. Here, there was no taking advantage.[236]

8.2.2 Governance by Contract and Promises

8.2.2.1 FTC Safeguards

1. FTC **Privacy Rule**: must have a clear statement of policy to customers and consumers.

2. FTC **Safeguards Rule**: must have a written information security plan describing a program to protect customer information.

8.2.2.2 Privacy Statements—Not Contracts: *In re Northwest Airlines Privacy Litigation*

Privacy statements are not contracts. The company can retain discretion to determine when the information is "relevant" and when "third parties" might need access.

1. After 9/11, Northwest began giving Passenger Name Records ("PNRs") to NASA. Plaintiffs brought multiple claims.

2. ECPA:[237]

   (a) § 2701: no. It prevent improper *access* but not improper disclosure.

   (b) § 2702: no. Northwest was not an electronic communications service provider.

3. Trespass: no. The PNRs were not plaintiffs' property.

4. Intrusion upon seclusion? No. There was no intrusion because plaintiffs voluntarily conveyed the information.

5. Contract/warranty? No.

[236] Casebook p. 807.
[237] Casebook p. 814–15.

8.2.2.3 Triggers for FTC Enforcement

1. Inadequate security.
2. Data breach due to negligence or failure to train employees.
3. Broken promises.
4. Retroactive privacy policy changes.
5. Deceptive data collection.
6. Inadequate disclosure of data gathering activities.

8.2.2.4 FTC Enforcement: *In the Matter of Google, Inc.*

1. Google's agreement with Gmail users promised that it would seek consent before using the data for other purposes.
2. Google's use of the data for Buzz without consent was a deceptive practice.[238]
3. Order: see casebook pp. 824–26. Includes the establishment of a "comprehensive privacy program" and 20 years of reporting.

8.2.2.5 Google settlement in the Safari matter

1. Google promised not to track Safari users that had opted out of third-party cookies, but then it circumvented the Safari cookie settings.[239]
2. Google and the FTC reached a $22.5 settlement (see below).

8.2.2.6 District Court order accepting the Google/FTC settlement

1. Google denies any violation, but agrees to (1) pay a $22.5 million fine, delete cookies on Safari browsers, and report on compliance to the FTC.

8.2.3 Governance by Statutory Regulation

8.2.3.1 VPPA I: *Dirkes v. Borough of Runnemede*

1. Anyone in possession of information that was improperly released is liable under VPPA—but see *Daniel* below.[240]

8.2.3.2 VPPA II: *Daniel v. Cantell*

1. Only video tape service providers are liable under VPPA.[241]

[238] Casebook p. 823 ff.
[239] See `http://www.ftc.gov/opa/2012/08/google.shtm`.
[240] Casebook p. 841.
[241] Casebook p. 845.

8.2.3.3 Cable Communications Policy Act

1. Applies to cable operators and service providers.[242]

8.2.3.4 Children's Online Privacy Protection Act

1. Passed in 1998.[243]
2. Safe harbor: no COPPA liability if the provider follows guidelines published by an FTC-approved group.[244]
3. After Dec. 2012: tracking of persistent identifiers of children is now a violation of COPPA—even if the site doesn't know the identity of the child.
   (a) So: how do you define PII under COPPA? How does it vary from the definition in other areas?

8.2.3.5 The Concept of PII

1. We lack a uniform definition.
2. Three approaches:[245]
   (a) Tautological: PII identifies people.
   (b) Non-public: any non-public information is personally identifying.
   (c) Specific types: list data fields that count as PII.
3. Paul Ohm: abandon PII.[246]
4. Solove and Schwartz: identifiability (and risk) is a continuum. More identifiability means more risk.
5. FTC staff report: when is information not "reasonably linkable" to a person?—When companies do not re-identify it.
6. Takeaway: lots of legal uncertainty about the definition of PII, here and abroad. EU may have broader definitions.

[242] Casebook p. 846.
[243] Casebook p. 847.
[244] Casebook p. 848.
[245] Casebook p. 873.
[246] Casebook p. 877.

8.2.3.6 Zip Codes as PII: *Pineda v. Williams-Sonoma Stores* ZIP codes are PII because they can be used in reverse searches.

1. Song-Beverly Credit Card Act (CA 1971): businesses can't collect PII while conducting credit card transactions.
   (a) Exceptions: can be used to prevent fraud, theft, or identity theft (e.g., at gas stations).
2. ZIP codes are PII under Song-Beverly because they can be used in reverse searches and they are not necessary to physical credit card transactions.[247]

8.3 Data Security

8.3.1 Data Security Breach Notification Statutes

1. California was the first after the ChoicePoint breach; now, almost all states have them.

8.3.2 Civil Liability

8.3.2.1 *Pisciotta v. Old National Bancorp*

1. After a data breach, plaintiffs requested damages for the cost of credit monitoring services. The court held that there had been no actual compensable injury. There were only "allegations of increased risk of future identity theft . . . ."[248]

8.3.3 FTC Regulation

8.3.3.1 FTC TRENDnet Settlement and Order

1. TRENDnet sold IP cams. It implemented faulty security, allowing hackers to access cameras that users thought were private.
2. TRENDnet was ordered to:
   (a) Implement a "comprehensive security program."
   (b) Get third-party assessments and submit reports for 20 years.
   (c) Notify affected customers.
   (d) File a report detailing compliance.

[247] Casebook p. 873. See also `http://www.sidley.com/California-Supreme-Court-Decides-Song-Beverly-Credit-Card-Act-of-1971-Does-Not-Apply-to-Online-Transactions-02-` (S-B act does not apply to online transactions).
[248] Casebook p. 887.

§ 9 International Privacy Law

9.1 OECD Guidelines

1. U.S. is a member.[249]
2. Enacted 1980. Grew out of a need for greater interoperability among international privacy frameworks.
3. Guidelines are **not binding anywhere**.
4. Guidelines:
   (a) Collection limitation.
   (b) Data quality.
   (c) Purpose specification.
   (d) Use limitation.
   (e) Security safeguards.
   (f) Openness/transparency.
   (g) Individual participation.
   (h) Accountability.
5. 2013: OECD adopts a revised recommendation.
6. Accountability requires a "privacy management program."
7. Notification is required for significant data breaches that are likely to have adverse effects.

9.2 Privacy Protection in Europe

9.2.1 Whitman, *The Two Western Cultures of Privacy: Dignity vs. Liberty*

1. United States: freedom from governmental intrusion; personal sovereignty—e.g., no national ID system.[250]
2. Europe: personal dignity, respect, honor, face-saving—e.g., no intrusive credit reports.

9.2.2 European Convention on Human Rights Article 8

1. EU: PII is all information **identifiable** to a person.
2. "Everyone has the right to respect for his private and family life, his home, and his correspondence."
3. Paul Schwartz: part of human dignity is being undignified.

[249] Casebook p. 1063–65 ff.
[250] Casebook p. 1065–70.

9.2.2.1 Facts vs. Intimate Details: *Von Hannover v. Germany*

1. Distinction between reporting facts and reporting intimate details.
2. Publication does not contribute to any debate of general interest to society.

9.2.2.2 "Wide Margin of Appreciation": *Mosley v. The United Kingdom*

States have a "wide margin of appreciation" in deciding how to "respect" Article 8. They can strike their own balance between privacy protections and freedom of expression. Here, there was no need for a press pre-notification requirement.

1. " . . . applicant was hardly exaggerating when he said that his life was ruined."[251]
2. States have a "wide margin of appreciation" in deciding how to "respect" Article 8.
3. Mosley sought press pre-notification requirement. The court rejected his request because Article 8 is about letting states adopt their own balance between privacy protections and freedom of expression.
4. Follow-up: a lower French court ordered Google to remove the Mosley photos.

9.2.3 The European Union Data Protection Directive (1995)

1. "Data protection law" (EU) = "information privacy law" (US).
2. Goals:
   (a) Free flow of information.
   (b) Protect fundamental rights.
   (c) Protect EU citizens' privacy worldwide.
3. Has shaped privacy law worldwide; the US is an outlier.
4. Emphases (i.e., FIPs):
   (a) Limits on collection.
   (b) Data quality principle.
   (c) Notice, access, and correction rights for individuals.
   (d) EU exclusive ideas:

[251] Casebook p. 1084.

i. Must have a legal basis to process information (inverse of US approach)—though consent can form a legal basis.
ii. Regulation by an independent data protection authority.
iii. Restrictions on data exports.
iv. Limits on automated decisionmaking.
v. Additional protections for sensitive data.

5. Allows data export only to countries with adequate protections. The **US does not have adequate protection** according to the EU.

6. Possible EU–US solutions:

   (a) Safe harbor standards that US companies could voluntarily follow.

   (b) Model contractual clauses. (Don't reinvent the wheel. Mental economy.)

   (c) Binding corporate rules.