Information Privacy Law

Joseph Mornin
Berkeley Law School
joseph@mornin.org

Fall 2013
Prof. Schwartz

Contents

§ 1 Introduction to Information Privacy Law

1.1 Information Privacy, Technology, and the Law

1.1.1 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.[1]

1.2 Information Privacy Law: Origins and Types

1.2.1 Common Law

1.2.1.1 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."[2]

2. Defamation doesn't protect "injury to the feelings."[3]

3. Intellectual property protections—for instance, the right to prevent publication—are part of a broader common law right to privacy.[4]

4. There is a "general right of the individual right of the individual to be let alone."[5] Invasion of privacy is a common law tort.[6]

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).[7]

1.2.1.2 Four Privacy Torts: Prosser, *Privacy*

1. Intrusion.[8]

2. Disclosure.

3. False light.

4. Appropriation.

---

[1] Casebook pp. 5–6.
[2] Casebook p. 14.
[3] Casebook p. 15.
[4] Casebook pp. 15–16.
[5] Casebook p. 18.
[6] Casebook pp. 18-20.
[7] Casebook p. 21.
[8] Casebook p. 27.

1.2.1.3 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).[9]

1.2.1.4 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.

1.2.2 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.

1.2.3 Statutory Law

1. Federal: many specific statutes.[10] Also, the general Privacy Act of 1974.
2. State: many specific statutes, but less than a third have enacted "omnibus data protection laws."[11]

1.2.4 International Law

1. OECD guidelines, APEC Privacy Framework.[12]

[9] Casebook pp. 29–31.
[10] See casebook pp. 36–39.
[11] Casebook p. 39.
[12] Casebook pp, 39–40.

1.3 Perspectives on Privacy

1.3.1 Philosophy

1.3.1.1 The Concept of Privacy and the Right to Privacy

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

1.3.1.2 The Public and Private Spheres

1. Arendt, Mill.[13].

1.3.2 Definition and Value

1.3.2.1 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.[14]

1.3.2.2 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."[15]

1.3.2.3 Solove, *Conceptualizing Property*

1. "When we state that we are protecting "privacy," we are claiming to guard against disruptions to certain practices."[16]
2. Privacy depends on context; there is no common denominator.[17]
3. Reductionists: privacy can be reduced to other concepts and rights.[18]

1.3.2.4 Allen, *Coercing Privacy*

1. Privacy is a "foundation, a precondition of a liberal egalitarian society."[19] So we should sometimes force it on people—for instance, through public nudity laws.

[13] Casebook pp. 40–41.
[14] Casebook pp. 42–45.
[15] Casebook pp. 48-49.
[16] Casebook p. 52.
[17] Casebook p. 53.
[18] Casebook p. 54.
[19] Casebook p. 55.

1.3.2.5 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.[20]

1.3.2.6 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.[21]

1.3.3 Critics

1.3.3.1 Posner, *The Right of Privacy*

1. Gossip can inform. Many people present themselves deceptively, so nosiness can be helpful.[22]

1.3.3.2 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).[23]

2.

1.3.4 Feminism and Privacy

1.3.4.1 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.

1.3.4.2 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.[24]

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

1. Privacy can perpetuate subordination.[25]

[20] Casebook p. 57.
[21] Casebook pp. 59–61.
[22] Casebook pp. 62–63.
[23] Casebook pp. 66–68.
[24] Casebook pp. 72–74.
[25] Casebook pp. 74–75.

1.3.4.4 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 . . . "[26]

[26] Casebook pp. 75–76.

§ 2 Privacy and the Media

2.1 Information Gathering

2.1.1 Intrusion upon Seclusion

2.1.1.1 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.

2.1.1.2 *Nader v. General Motors Corp.*

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.[27]
4. Held: Nader's allegations were sufficient to withstand a motion for summary judgment.[28]
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."[29]

2.1.1.3 Private Spaces: *Dietemann v. Time, Inc.*

1. Dietemann was practicing quack medicine in his home (cf. *Desnick* below). A Time reporter secretly recorded a session and later published a story.
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 . . . ."[30]
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."[31]

[27] Casebook p. 81.
[28] Casebook p. 82.
[29] Casebook p. 83.
[30] Casebook p. 87.
[31] Casebook p. 87.

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

Professionals assume the risk that their clients will publicize their interactions.

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."[32]

2.1.1.5 *Food Lion, Inc. v. ABC*

2.1.1.6 *Shulman v. Group W Productions, Inc.*

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.[33]
2. Upon broadcast, Shulman sued for unlawful intrusion and public disclosure of private facts.
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."[34]
7. Reversed.

[32] Casebook p. 90.
[33] Casebook pp. 94–96.
[34] Casebook p. 97.

2.1.2 Paparazzi

2.1.2.1 *Galella v. Onassis*

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.[35]
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 . . . ."[36]

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

1. The Act defines two forms of invasion of privacy:[37]
   (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.[38]
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:[39]

[35] Casebook p. 99.
[36] Casebook p. 100.
[37] Casebook p. 101.
[38] Casebook p. 102.
[39] Casebook pp. 104–06.

(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.

2.1.3 Video Voyeurism

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

2.1.3.1 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.[40]

2.2 Disclosure of Truthful Information

1. What types of disclosure should trigger civil liability?

2. How can liability for disclosure coexist with the First Amendment?

2.2.1 Public Disclosure of Private Facts

2.2.1.1 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.[41]

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

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.'"[42]

[40] Casebook pp. 107–108.
[41] Casebook p. 110.
[42] Casebook p. 111.

3. The photograph only "extended knowledge of the particular incident to a somewhat larger public than actually witnessed it at the time of occurrence."[43]

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.[44]

2.2.1.3 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.[45]

2. The newspaper argued that the photo was "a matter of legitimate news interest to the public . . . ."[46]

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."[47]

5. Commentary:

   (a) Courts vary in the privacy protections they give to information disclosed to small groups of people.[48] 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.[49]

   (b) Someone who gives comments to journalists can retract consent before publication.[50] Media entities can disseminate already public information, but further disclosure can lead to liability.[51]

[43] Casebook p. 112.
[44] Casebook p. 112.
[45] Casebook p. 115.
[46] Casebook p. 115.
[47] Casebook p. 116.
[48] Casebook p. 117–18.
[49] Casebook pp. 118–19.
[50] Casebook p. 119.
[51] Casebook p. 120.

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

What are the boundaries of "the public"? Can it be a small group?

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."[52]
4. (Many courts, and possibly the Restatement, disagree.[53])
5. Commentary:
   (a) The widespread publicity requirement singles out broadcast media for restraints that don't apply to "gossip-mongers."[54]
   (b) We often care more what a small group thinks of us.

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

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.[55]
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"[56] knew that Sipple was gay) and (2) the facts were newsworthy because they were "prompted by legitimate political considerations"[57] (e.g., did Ford fail to publicly thank Sipple because of bias against gays?).

2.2.1.6 What is newsworthy?

1. Courts use three tests:[58]
   (a) **Defer to editorial judgment** and make no distinction between news and entertainment.

[52] Casebook p. 121.
[53] Casebook pp. 122–23.
[54] Casebook p. 123.
[55] Casebook p. 123–24.
[56] Casebook p. 125.
[57] Casebook p. 126.
[58] Casebook p. 128.

   (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?)[59]

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."[60]

   (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.

4.

2.2.1.7 Newsworthiness Test II: *Shulman v. Group W Productions*

2.2.1.8 Newsworthiness Test III: *Bonome v. Kaysen*

2.2.2 First Amendment Limitations

2.2.2.1 *Cox Broadcasting Corp. v. Cohn*

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.[61]

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.[62]

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:[63]

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

[59] Casebook p. 129.
[60] Casebook p. 130.
[61] Casebook pp. 148–49.
[62] Casebook p. 150.
[63] Casebook pp. 150–51.

(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."

2.2.2.2 *Shulman v. Group W. Productions, Inc.*

2.2.2.3 *Bartnicki v. Vopper*

2.3 Dissemination of False or Misleading Information

2.3.1 Defamation

2.3.1.1 *Blumenthal v. Drudge*

2.3.1.2 *Barrett v. Rosenthal*

2.3.1.3 *Batzel v. Smith*

2.3.1.4 Siegenthaler and Wikipedia

2.3.1.5 Actual Malice: *New York Times v. Sullivan*

To recover for defamation, public officials must prove actual malice.

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:

   (a) Can courts impose liability for libel against public officials in their public capacity without abridging constitutionally protected speech?[64]

   (b) The speech here was constitutionally protected, but does it "forfeit[] that protection by the falsity of its statements . . . "?[65]

   (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 . . . . "[66]

[64] Casebook p. 195.
[65] Casebook p. 196.
[66] Casebook p. 196.

3. Other Justices argued that defamation should be eliminated altogether for public officials, since the truth will emerge in the marketplace of ideas.[67]

2.3.1.6 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.[68]
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.[69]
   (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."[70]
   (d) Held: states can determine for themselves the standard of liability for defamation that injures private citizens.[71]
   (e) However, punitive damages require a showing of actual malice. Otherwise, juries might "use their discretion to punish expressions of unpopular views."[72] 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.[73]

[67] Casebook p. 197.
[68] Casebook p. 198.
[69] Casebook p. 199.
[70] Casebook p. 199.
[71] Casebook p. 200.
[72] Casebook p. 200.
[73] Casebook p. 201.

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

1. The court opinion in the Firestones' divorce described the couple's many "extramarital escapades."[74] *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* . . . . "[75]

2.3.1.8 *Wolston v. Readers Digest Ass'n, Inc.*

2.3.1.9 *Atlanta Journal-Constitution v. Jewell*

2.3.1.10 *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*

2.3.2 False Light

2.3.2.1 Overview

2.3.2.2 *Time, Inc. v. Hill*

2.3.3 Infliction of Emotional Distress

2.3.3.1 *Hustler Magazine v. Falwell*

2.3.3.2 *Snyder v. Phelps*

2.4 Appropriation of Name or Likeness

2.4.0.3 Introduction

1. Appropriation: privacy-based; concerned with dignity.

2. Right of publicity: property-based; concerned with commercial reward.[76]

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

Appropriation of identity can occur without using a name or likeness.

1. Carson brought two actions, based on the right to privacy and the right to publicity.

[74] Casebook p. 202.
[75] Casebook p. 202.
[76] Casebook p. 221.

2. Right to privacy: this tort is based on embarrassment, but there is no evidence here that Carson was embarrassed.[77]

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.[78]

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.[79]

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

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.[80]

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

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.[81]

   (a) TODO what about the fact that most news organizations are also commercial entities? and that the need to earn a profit is a major factor in what they decide to report on?

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."[82]

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.[83]

[77] Casebook p. 233.
[78] Casebook p. 234.
[79] Casebook pp. 225–27.
[80] Casebook p. 231.
[81] Casebook p. 233.
[82] Casebook p. 234.
[83] Casebook pp. 235–36.

2.4.0.7 First Amendment Limitations: *Zacchini v. Scripps-Howard Broadcasting Co.*

The appropriation tort does not violate the First Amendment.

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.[84]
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*):[85]
   (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.[86]

2.4.0.8 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.[87]
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 . . . ."[88]

[84] Casebook p. 239.
[85] Casebook p. 240.
[86] Casebook p. 240.
[87] Casebook p. 242.
[88] Casebook p. 244.

§ 3 Privacy and Law Enforcement

3.1 The Fourth Amendment and Emerging Technology

3.1.1 Introduction

1.

3.1.2 Wirtetapping, Bugging, and Beyond

3.1.2.1 *Olmstead v. United States*

1.

3.1.2.2 *Lopez v. United States*

1.

3.1.2.3 *Katz v. United States*

1.

3.1.2.4 *United States v. White*

1.

3.1.3 The Reasonable Expectation of Privacy Test and Emerging Technology

3.1.3.1 *Smith v. Maryland*

1.

3.1.3.2 *United States v. Place*

1.

3.1.3.3 *Illinois v. Caballes*

1.

3.1.3.4 *California v. Greenwood*

1.

3.1.3.5 Plain View, Open Fields, and Curtilage

1.

3.1.3.6 *Florida v. Riley*

1.

3.1.3.7 *Dow Chemical v. United States*

1.

3.1.3.8 *Kyllo v. United States*

1.

3.2 Federal Electronic Surveillance Law

3.2.1 Section 605 of the Federal Communications Act

1.

3.2.2 Title III

1.

3.2.3 The Electronic Communications Privacy Act

1.

2.

3.2.4 The Communications Assistance for Law Enforcement Act

1.

3.2.5 The USA PATRIOT Act

1.

3.3 Digital Searches and Seizures

3.4 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 storage" under the Wiretap Act does not include stored data.

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.[89]

[89] Casebook pp. 345–46.

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)[90]?

   (a) No. "'Electronic communication" does not include electronic storage of such communications."[91]

4. However, the Secret Service is liable under the SCA.[92]

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

1. Does the Fourth Amendment protect stored emails?[93]

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.

3.4.2 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.

2. Emails are private, just like letters.[94]

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.[95]

4. The SCA is unconstitutional to the extent that it lets government compel ISPs to turn over email contents without a warrant.[96]

[90] Anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."
[91] Casebook pp. 346–47.
[92] § 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."
[93] Casebook pp. 348–49.
[94] Casebook p. 352–53.
[95] Casebook p. 354–55.
[96] Casebook p. 355.

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."[97]

3.4.3 ISP Records: *United States v. Hambrick*

1. An undercover detective subpoenaed an ISP to get subscriber data for someone posting criminal messages in a chat room. The subpoena was invalid.

2. The defendant argued that ECPA creates a Fourth Amendment REOP in subscriber data. The court disagreed.[98]

3. There is no exclusionary rule here; civil damages are the only remedy.

3.4.4 *McVeigh v. Cohen*

- navy used social engineering to get info from aol - navy "asked" without mcveigh "telling"; mcveigh had a privacy expectation in his online activity. i.e., his online activity didn't count as "telling" under DADT. - court granted a suppression remedy [?] bc gov't solicited [?] aol to break the law. pp. 363–64.

3.4.5 IP Addresses and URLs: *U.S. v. Forrester*

- surveillance here: analogous to pen register; and no suppression remedy under the pen register act

3.4.6 Keylogging: *United States v. Scarfo*

3.5 National Security and Foreign Intelligence

3.5.1 Is National Security Different? *United States v. United States District Court* (the *Keith* case)

1.

3.5.2 Foreign Intelligence Surveillance Act (FISA)

3.5.2.1 *Global Relief Foundation, Inc. v. O'Neil*

1.

[97] Casebook p. 352.
[98] Casebook pp. 358–59.

3.5.2.2 *United States v. Isa*

1.

3.5.2.3 *The 9/11 Commission Report*

1.

3.5.2.4 *In re Sealed Case*

1.

3.5.3 Attorney General's FBI Guidelines

1.

3.5.4 NSA Surveillance Program

3.5.4.1 Overview

1.

3.5.4.2 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.

3.5.4.3 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.

3.5.5 *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."[99]

iv. The alleged injuries here are different than other standing cases on which the respondents rely.[100]

3. Justice Breyer, dissenting:

(a) The question was whether the injury was "actual or imminent."[101]

(b) There is a high likelihood that under § 1881(a) the government will intercept some of the plaintiffs' communications.[102] The harm is not "speculative."[103]

[99] 2.
[100] 3.
[101] 2.
[102] 6, 9.
[103] 10.

§ 4 Health Privacy

4.1 Confidentiality of Medical Information

1. HIPAA: 1996. HHS regulations implementing HIPAA: November 1999.
2. **Privacy rule** (2000): final version of HIPAA regulations.[104] 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.[105]

4.2 Constitutional Protection of Medical Information

4.2.1 *Whalen v. Roe*

1.

4.2.2 42 U.S.C. § 1983 and "Constitutional Torts"

1.

4.2.3 *Carter v. Broadlawns Medical Center*

1.

4.2.4 *Doe v. Borough of Barrington*

1. Police officers revealed to the defendant's neighbors the fact that he was HIV positive.[106]
2. Held: the Constitution protects against government disclosure of HIV status.[107] The state must show a compelling government interest to disclose HIV status.[108]

[104] Casebook p. 463.
[105] Casebook p. 475.
[106] Casebook p. 513.
[107] Casebook p. 514.
[108] Casebook p. 515.

4.2.5 *Doe v. Southeastern Pennsylvania Transportation Authority*

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.[109]

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.[110]

3. *Westinghouse*: seven factors to determine whether disclosure is actionable.

4. Held: the intrusion here was minimal. On balance, the employer's interests are more substantial.[111]

5.

4.3 Genetic Information

4.3.1 Overview

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

2.

3.

4.

4.3.2 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.

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.[112]

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.

[109] Casebook pp. 516–18.
[110] Casebook p. 519.
[111] Casebook p. 521.
[112] See slip opinion.

(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.)

§ 5 Privacy and Government Records and Databases

5.1 Public Access to Government Records

5.1.1 Public Records and Court Records

5.1.1.1 *Doe v. Shakur*

1.

5.1.2 The Freedom of Information Act

5.1.2.1 *DOJ v. Reporters Committee for Freedom of the Press*

1.

5.1.2.2 *NARA v. Favish*

1.

5.1.3 Constitutional Limitations on Public Access

5.1.3.1 *Paul v. Davis*

1.

5.1.3.2 *Cline v. Rogers*

1.

5.1.3.3 *Scheetz v. The Morning Call, Inc.*

1.

5.2 Government Records of Personal Information

5.2.1 Fair Information Practices

5.2.1.1 Marc Rotenberg, Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)

1.

5.2.2 The Privacy Act

5.2.2.1 *Quinn v. Stone*

1.

5.2.2.2 *Doe v. Chao*

1.

5.2.3 The Driver's Privacy Protection Act

§ 6 Privacy of Financial and Commercial Data

6.1 The Financial Services Industry and Personal Data

6.1.1 Fair Credit Reporting Act

1. 1970: FCRA.
2. Scope turns on the definition of "consumer report." Most reports dealing with consumer credit fall within this definition.[113]
3. Statutory requirements: see casebook pp. 758–65.

6.1.1.1 *Smith v. Bob Smith Chevrolet, Inc.*

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.[114]
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 wilfully violated FCRA.[115]
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.[116]
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.[117]
5. Whether Bob Smith's noncompliance was wilful was a jury question.[118]

6.1.1.2 *Sarver v. Experian Information Solutions*

6.1.2 The Use and Disclosure of Financial Information

6.1.2.1 The Breach of Confidentiality Tort and Financial Institutions

1.

[113] Casebook p. 758.
[114] Casebook p. 765–77..
[115] Casebook p. 766.
[116] Casebook p. 767-68.
[117] Casebook p. 768–69..
[118] Casebook p. 769.

6.1.2.2 The Graham-Leach-Bliley Act

1.

6.1.2.3 State Financial Regulation

1.

6.1.3 Identity Theft

6.1.3.1 Identity Theft Statutes

1. Identity Theft Assumption and Deterrence Act: federal, 1998.[119]
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.[120]

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

Identity theft is foreseeable and preventable, so banks have to implements 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.[121]
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.[122]
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.[123]

6.1.3.3 FCRA: *Sloane v. Equifax*

1.

[119] Casebook p. 786.
[120] Casebook p. 787–88..
[121] Casebook p. 789.
[122] Casebook p. 790.
[123] Casebook p. 791.

6.2 Commercial Entities and Personal Data

6.2.1 Governance by Tort

6.2.1.1 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.[124]
2. Intrusion upon seclusion:
   (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.[125]
   (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.[126]
3. Is there harm in knowing patterns of consumption? See pp. 802–04.

6.2.1.2 Private Investigators: *Remsberg v. Docusearch, Inc.*

1. Youens hired Docusearch to get Boyer's personal information. Docusearch lied to get some of the information. Youens later found and killed Boyer.[127]
2. Private citizens generally have no duty to protect others from the criminal acts of third parties.[128] 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.

[124] Casebook p. 799.
[125] Casebook p. 800.
[126] Casebook p. 801.
[127] Casebook p. 804.
[128] Casebook p. 805.

3. Stalking and identity theft are foreseeable.[129]

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.

   (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.[130]

6.2.2 Governance by Contract and Promises

6.2.2.1 *In re Northwest Airlines Privacy Litigation*

Airlines are not prohibited from disclosing passenger records to government agencies.

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

2. ECPA:[131]

   (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.

6.2.2.2 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.

[129] Casebook p. 806.
[130] Casebook p. 807.
[131] Casebook p. 814–15.

2. Google's use of the data for Buzz without consent was a deceptive practice.[132]

3. Order: see casebook pp. 824–26. Includes the establishment of a "comprehensive privacy program" and 20 years of reporting.

6.2.2.3 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.[133]

2. Google and the FTC reached a $22.5 settlement (see below).

6.2.2.4 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.

6.2.3 Governance by Statutory Regulation

6.2.3.1 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.[134]

6.2.3.2 VPPA II: *Daniel v. Cantell*

1. Only video tape service providers are liable under VPPA.[135]

6.2.3.3 Cable Communications Policy Act

1. Applies to cable operators and service providers.[136]

6.2.3.4 Children's Online Privacy Protection Act

1. Passed in 1998.[137]

2. Safe harbor: no COPPA liability if the provider follows guidelines published by an FTC-approved group.[138]

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?

[132] Casebook p. 823 ff.
[133] See `http://www.ftc.gov/opa/2012/08/google.shtm`.
[134] Casebook p. 841.
[135] Casebook p. 845.
[136] Casebook p. 846.
[137] Casebook p. 847.
[138] Casebook p. 848.

6.2.3.5 The Concept of PII

1. We lack a uniform definition.
2. Three approaches:[139]
   (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.[140]
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.

6.2.3.6 *Pineda v. Williams-Sonoma Stores*

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.[141]

6.3 Data Security

6.3.1 Data Security Breach Notification Statutes

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

6.3.2 Civil Liability

6.3.2.1 *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 . . . ."[142]

[139] Casebook p. 873.
[140] Casebook p. 877.
[141] 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).
[142] Casebook p. 887.

6.3.3 FTC Regulation

6.3.3.1 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.

§ 7 International Privacy Law

7.1 OECD Guidelines

1. U.S. is a member.[143]
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.

7.2 Privacy Protection in Europe

7.2.1 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.[144]
2. Europe: personal dignity, respect, honor, face-saving—e.g., no intrusive credit reports.

[143] Casebook p. 1063–65 ff.
[144] Casebook p. 1065–70.

7.2.2 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.
4. Paul Schwartz: part of human dignity is being undignified.

7.2.2.1 Privacy and the Media: *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.
3.

7.2.2.2 Privacy and the Media: *Mosley v. The United Kingdom*

1. " . . . applicant was hardly exaggerating when he said that his life was ruined."[145]
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.
5.

7.2.3 The European Union Data Protection Directive (1995)

7.2.3.1 Introduction

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.

[145] Casebook p. 1084.

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:
      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.

7.2.3.2 *Criminal Proceedings against Bodil Lindqvist*

1.

7.2.3.3 Article 8 and Harmonization

1.

7.2.3.4 Supervisory Authority and Individual Remedies

1.