Update – Fall 2007

INFORMATION PRIVACY LAW
2nd Edition
(Aspen Publishing Co. 2006)

by

Daniel J. Solove
Associate Professor of Law
George Washington University Law School

Marc Rotenberg
Executive Director
The Electronic Privacy
Information Center
&
Adjunct Professor of Law
Georgetown University Law Center

Paul M. Schwartz
Professor of Law
U.C. Berkeley School of Law

The Fall 2007 Update was prepared by
Daniel J. Solove & Paul M. Schwartz

We would like to thank Fred Cate, Steven McDonald, Lior Strahilevitz, and Peter Winn for their helpful comments on the last edition of the casebook and for their suggestions for this update.

A new edition of the book is in the works for 2009. We anticipate it being ready late in the year in 2008, so it can be used in spring 2009 classes.
CHAPTER 1: INTRODUCTION

SUMMARY OF ADDITIONS TO CHAPTER

• No new changes or additions.
## SUMMARY OF ADDITIONS TO CHAPTER

- In B.1(d) (the newsworthiness test element of the public disclosure tort), we added an excerpt from *Bonome v. Kaysen*.

- Extensive notes following *Bonome v. Kaysen* examine the applicability of the public disclosure tort to Internet gossip in blogs and social network websites.

- In B.2 (disclosure of illegally obtained information), we added a note discussing *Boehner v. McDermott* after the excerpt of *Bartnicki v. Vopper*. *Boehner* is a new case that interprets and distinguishes *Bartnicki*.

- In C.1(d) (defamation on the Internet), we added notes discussing more cases applying the CDA § 230, including *Barrett v. Rosenthal*, *Yahoo! v. Barnes*, and *Batzel v. Smith*. A new note discusses the applicability of § 230 to Wikipedia.

- In D (appropriation), we added a new section addressing the element of “for one’s own use of benefit” including an excerpt from *Raymen v. United Senior Association, Inc.*. Notes to the case explore the fuzzy line between commercial and non-commercial uses as well as excerpts from cases involving Girls Gone Wild videos.

## B. DISCLOSURE OF TRUTHFUL INFORMATION

### 1. PUBLIC DISCLOSURE OF PRIVATE FACTS

#### (d) The Newsworthiness Test

p. 131 – Add the following case and notes & questions before section (e):

**Bonome v. Kaysen**


Muse, J. Joseph Bonome filed this action alleging invasion of privacy against Susana Kaysen, the author of a memoir at the center of this case, and Random House, Inc., the publisher.

In the early 1990s, Bonome owned and operated a tree surgery and landscaping business primarily in the Cambridge, Massachusetts area. At the time, he was living in New Hampshire and was married with step-children. Kaysen was an author living in Cambridge. She had gained success and notoriety for her book *Girl, Interrupted* which was made into what has been described to be a critically acclaimed film. In 1994, Bonome met Kaysen and the two began having an affair, including a physical...
relationship. Kaysen pressured Bonome to leave his wife, and Bonome ultimately succumbed to that pressure. Bonome divorced his wife in 1996 and shortly thereafter moved into Kaysen’s home, where they continued the relationship.

Within six months or a year into the relationship, Kaysen began to experience severe vaginal pain. She began to regularly see doctors for her problem, but over the course of several years was unable to receive sufficient curative treatment. During this time period, she began working on a new book, which book is the subject of this case. Despite Bonome’s inquiries, Kaysen would not reveal the subject of the book to him.

The fact of their relationship was well-known to Bonome’s family, friends, and clientele. However, the details of their physical relationship were private. Bonome’s parents and three brothers all spent time, including some holidays, with the couple. However, in July 1998, the relationship “ended” when Kaysen asked Bonome to move out, which he did. Despite the breakup, their physical relationship continued for at least three months longer.

In 2001, Random House published the book *The Camera My Mother Gave Me*. The book only refers to Bonome as Kaysen’s “boyfriend” and alters details about his life—such as where he was from, and his occupation. The book is an autobiographical memoir chronicling the effects of Kaysen’s seemingly undiagnosable vaginal pain in a series of ruminations about the condition’s effects on many aspects of her life, including her overall physical and emotional state, friendships, and her relationship with her boyfriend. It details her intense pain and discomfort and her many fruitless attempts to obtain an accurate medical diagnosis and effective treatment.

One of the central themes of the book concerns the impact of her chronic pain on the emotional and physical relationship with Kaysen’s boyfriend. To that end, the book details, graphically on a few occasions, several sexual encounters between them. It portrays the boyfriend as becoming increasingly frustrated and impatient with Kaysen’s condition and her reluctance and/or refusal to engage in physical intimacy. The boyfriend is described as “always bugging [her] for sex” and “whining and pleading” for sex, as well as being ignorant and insensitive to her emotional and physical state. In this vein, it attributes many aggressive and overtly offensive sexual quotes to him. Ultimately, the development of this theme culminates in a scene where the boyfriend is physically forceful in an attempt to engage her in sex. This scene is followed by ruminations about whether the relationship had exceeded the bounds of consensual sexual relations into the realm of coerced non-consensual sex. . . .

After publication of the book, Bonome learned that many local friends and family had read the book and understood the portrayal of the “boyfriend” to be a depiction of him. In addition, Bonome’s business clientele included friends of Kaysen who also understood that Bonome was the “boyfriend.” As a result of the publication, Bonome has suffered severe personal humiliation, and his reputation has been severely damaged among a substantial percentage of his clients and acquaintances. . . .

General Laws chapter 214 Section 1B provides that: “[a] person shall have a right against unreasonable, substantial or serious interference with his privacy.” Section 1B has been interpreted to include the common-law tort of “public disclosure of private facts” as articulated in the Restatement (Second) of Torts. . . .
This case presents an additional challenge in that it pits Kaysen’s right of publicity-- her own right to disclose intimate facts about herself--directly in conflict Bonome’s right to control the dissemination of private information about himself.

Undoubtedly, the information revealed was of an intensely intimate and personal nature. Indeed, commentators and courts have almost universally recognized one’s sexual affairs as falling squarely within the sphere of private life.

Otherwise private information may properly be published when it is sufficiently related to a broader topic of legitimate public concern. In this case, a critical issue is whether the personal information concerning Bonome is in the book for its relevance to issues of legitimate public concern or is merely “morbid and sensational plying into [Bonome’s] private [life] for its own sake.”

After examining the statements concerning the boyfriend and their relevance to the broader themes of the book, it is clear that the details are included to develop and explore those themes. Specifically, the book explores the way in which Kaysen’s undiagnosed physical condition impacted her physical and emotional relationship with “her boyfriend.” Moreover, it explores the issue of when undesired physical intimacy crosses the line into non-consensual sexual relations in the context of her condition. These broader topics are all matters of legitimate public concern, and it is within this specific context that the explicit and highly personal details of the relationship are discussed. Thus, the defendants had a legitimate and protected interest to publish these facts.

As noted above, there is an additional interest in this case: Kaysen’s right to disclose her own intimate affairs. In this case, it is critical that Kaysen was not a disinterested third party telling Bonome’s personal story in order to develop the themes in her book. Rather, she is telling her own personal story-- which inextricably involves Bonome in an intimate way. In this regard, several courts have held that where an autobiographical account related to a matter of legitimate public interest reveals private information concerning a third party, the disclosure is protected so long as there is a sufficient nexus between those private details and the issue of public concern.

Where one’s own personal story involves issues of legitimate public concern, it is often difficult, if not impossible, to separate one’s intimate and personal experiences from the people with whom those experiences are shared. Thus, it is within the context of Bonome and Kaysen’s lives being inextricably bound together by their intimate relationship that the disclosures in this case must be viewed. Because the First Amendment protects Kaysen’s ability to contribute her own personal experiences to the public discourse on important and legitimate issues of public concern, disclosing Bonome’s involvement in those experiences is a necessary incident thereto.

The privilege to disclose private information is limited by the requirement that the disclosure bear the necessary nexus (both logical and proportional) to the issue of legitimate public concern. In this regard, it is of importance that Kaysen did not use Bonome’s name in the book. The defendants did not subject Bonome to unnecessary publicity or attention. The realm of people that could identify Bonome as the boyfriend are those close personal friends, family, and business clients that knew of the relationship. This is not to overlook or discount the impact this disclosure may have had on Bonome, or his substantial claim that Kaysen breached a fundamental trust of their relationship. However arguably odious, the defendants did not exercise the right of
disclosure in a manner offensive to the balance of those interests. See Restatement (Second) Torts § 652D, comment a (“Publicity ... means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge”).

This court is not unmindful of the injury claimed by Bonome, who alleges to have suffered personal humiliation within his familial circle, as well as with friends and business clientele as a result of the book’s publication. Nonetheless, Kaysen’s own personal story--insofar as it relates to matters of legitimate public concern--is hers to contribute to the public discourse. This right is protected by the First Amendment. Inasmuch as the book does not exceed the bounds of that constitutional privilege, Bonome’s claim for invasion of privacy under G.L.c. 214, § 1B is DISMISSED.

NOTES & QUESTIONS

1. The Right to Tell One’s Story. The newsworthiness test examines whether a disclosure is of “legitimate public concern.” It does not matter who is making the disclosure for the purposes of the test. However, the court suggests that “there is an additional interest in this case: Kaysen’s right to disclose her own intimate affairs.” The court states that “it is critical that Kaysen was not a disinterested third party telling Bonome’s personal story in order to develop the themes in her book. Rather, she is telling her own personal story--which inextricably involves Bonome in an intimate way.” Does the autobiographical nature of the disclosure change the newsworthiness analysis? Should it? Should a person have increased latitude when revealing private information about others when it also involves her own autobiographical details? Suppose Kaysen told her story to a journalist, who wrote about it in an article. Should the journalist receive less protection for making the disclosure than Kaysen would receive for revealing the same facts?

2. Blogs, Social Network Websites, and Gossip. In Steinbuch v. Cutler, 463 F. Supp. 2d 1 (D.D.C. 2006), Jessica Cutler, a staff member for a U.S. senator, wrote a blog about her relationships with several men, including a man she was dating who also worked for the senator. In her blog, The Washingtonienne, she described in vivid detail their budding romance, including their sexual activities. Specifically, Cutler described their sexual practices, conversations, and other intimate details. Cutler did not identify Steinbuch directly, but she used his real initials and disclosed other personally identifiable information that made it possible for him to be identified. For a few weeks, only a handful of people knew about Cutler’s blog. Then Wonkette, a very popular political gossip blog, linked to her blog and tens of thousands began flocking to the site. The story was written about in many major newspapers, and Cutler wrote a book based on the blog and posed for Playboy magazine. Robert Steinbuch, the attorney who worked for the same senator as Cutler, sued her for violating his privacy. The case ultimately never proceeded to trial because Cutler declared bankruptcy. Had the case proceeded further, how should it have been resolved? Should Bonome v. Kaysen control? Can it be distinguished, and if so, how?

One of Cutler’s arguments was that the blog was only read by a handful of her friends until it was linked to by Wonkette. She contended that she never gave widespread
publicity to the information – Wonkette did. When information is disclosed on the Internet, but only a few people read it, is disclosure sufficiently widespread for the publicity element to be satisfied?

Cutler also argued that her account of her relationships was newsworthy. According to her motion to dismiss: “Cutler’s Blog makes a shocking and disturbing portrayal of casual and even reckless sexual encounters between young, entry-level Capitol Hill staffers like Cutler and more senior staffers like Steinbuch. . . . . The interrelationship between youth, beauty, sex, money, and power in Washington has long been a matter of legitimate and sometimes pressing public interest.” Is Cutler’s blog newsworthy? What are the best arguments on each side of the issue?

In his book, The Future of Reputation, Daniel Solove observes that people are increasingly expressing themselves in blogs and social network websites such as MySpace and Facebook. People are revealing information about their private lives as well as gossip and rumors about their friends, family, co-workers, and others. Solove notes:

In the past, gossip occurred backstage; it was fleeting and localized. The anthropologist Sally Engle Merry observes: “Gossip flourishes in close-knit, highly connected social networks but atrophies in loose-knit, unconnected ones.” Before the rise of the blogosphere, Jessica Cutler’s gossip about her sexual experiences with Robert would probably have remained within her small circle of friends. But today details about people’s private lives are increasingly migrating to the Internet. Jessica’s blog was read by hundreds of thousands of people—perhaps millions. It is becoming harder and harder for people to escape their pasts. . . . Moreover, traditional gossip occurs in a context, among people who know the person being gossiped about. But the Internet strips away that context, and this can make gossip even more pernicious.

The Internet is transforming the nature and effects of gossip. It is making gossip more permanent and widespread, but less discriminating in the appropriateness of audience. . . . The problem with Internet gossip is that it can so readily be untethered from its context.

More broadly, Solove observes, the transformation of gossip from the fleeting and forgettable to the permanent and searchable might have significant social effects:

The Internet allows information to flow more freely than ever before. We can communicate and share ideas in unprecedented ways. These developments are revolutionizing our self-expression and enhancing our freedom.

But there’s a problem. We’re heading toward a world where an extensive trail of information fragments about us will be forever preserved on the Internet, displayed instantly in a Google search. We will be forced to live with a detailed record beginning with childhood that will stay with us for life wherever we go, searchable and accessible from anywhere in the world. This data can often be of dubious reliability; it can be false and defamatory; or it can be true but deeply humiliating or discrediting. We may find it increasingly difficult to have a fresh start, a second chance, or a clean slate. We might find it harder to engage in self-exploration if every false step and foolish act is chronicled forever in a permanent record. This record will affect our ability to define our identities, to obtain jobs, to participate in public life, and more. Ironically, the unconstrained flow of information on the Internet might impede our freedom. How and why is this happening? How can the free flow of information make us more free yet less free as well?¹

3. The Breach of Confidentiality Tort. As will be discussed in Chapter 4, the breach of confidentiality tort protects against the nonconsensual disclosures of

confidential information. Unlike the tort of public disclosure, the breach of confidentiality tort does not have the elements of highly offensive, publicity, or the newsworthiness test. In America, the breach of confidentiality tort has been applied to doctors and other professionals. In contrast, in England, which rejects the Warren and Brandeis privacy torts, including the public disclosure tort, has a robust breach of confidentiality tort. As Neil Richards and Daniel Solove note:

The law of confidentiality in England also has attributes that the American privacy torts lack. In America, the prevailing belief is that people assume the risk of betrayal when they share secrets with each other. But in England, spouses, ex-spouses, friends, and nearly anyone else can be liable for divulging confidences. As one English court noted: “The fact is that when people kiss and later one of them tells, that second person is almost certainly breaking a confidential arrangement.” Confidentiality thus recognizes that nondisclosure expectations emerge not just from norms of individual dignity, but also from norms of relationships, trust, and reliance on promises. American privacy law has never fully embraced privacy within relationships; it typically views information exposed to others as no longer private. Although a tort remedying breach of confidence would emerge later on in American law, it has developed slowly in comparison to the Warren and Brandeis privacy torts.2

Suppose the breach of confidentiality tort were applied more broadly to situations where friends, spouses, and others disclosed the secrets of others. Andrew McClurg notes that the First Amendment implications of the breach of confidentiality tort are different from those of the public disclosure tort:

If one accepts the proposition that a party to an intimate relationship impliedly agrees not the breach the other party’s confidence by publishing private, embarrassing information about them via an instrument of mass communication, the speech restriction is one that is self-imposed, rather than state-imposed.3

How might a broader application of the breach of confidentiality tort impact bloggers like Jessica Cutler who write about their sexual activities with others? Would the tort impair free speech too much? Note that there is no newsworthiness test under the tort, so information of public concern is not protected. On the other hand, as McClurg notes, the breach of confidentiality tort understands that parties have made an implicit contract of confidentiality. Is it a violation of free speech to enforce a person’s explicit or implicit promise not to speak about something?

4. Reputation-Tracking Technologies. Lior Strahilevitz argues that reputation-tracking technologies can yield beneficial results. He points to programs such as “How’s My Driving?” (HMD programs) in which some commercial vehicles have stickers with a number to call to complain about bad driving. Insurance company statistics reveal significant reductions in crash costs and accidents (declines well over 30%) following the implication of HMD programs. Strahilevitz argues that the reason for the effectiveness of HMD programs is that they reduce driver anonymity:

---


The problems associated with urban and suburban driving are, by and large, creatures of motorist anonymity. That statement may seem too bold to readers accustomed to hearing about drunken driving, drowsy driving, and road rage. But a review of the literature on driving suggests that these problems largely stem from roadway anonymity. If society were able to monitor its roadways around the clock and to analyze this data immediately to identify and punish problematic motorists, many of the traffic accident deaths that occur every year would be averted. A dangerous driving environment is the almost inevitable consequence of sporadic traffic law enforcement by the police combined with rare traffic norm enforcement by motorists.4

Strahilevitz points out that various websites such as Amazon.com, Tripadvisor.com, and eBay.com harness user feedback, where people can leave comments about a particular merchant or individual: “Though eBay’s reputation system is admittedly imperfect, it has been extraordinarily successful at preventing fraud among auction participants.” He proposes that more measures like HMD programs in other contexts might be beneficial. In what other situations would reputation-tracking technologies be useful? What are the potential problems with such technologies? Is there a way to implement these technologies that minimize these problems?

B. DISCLOSURE OF TRUTHFUL INFORMATION

1. PUBLIC DISCLOSURE OF PRIVATE FACTS
   (e) First Amendment Implications

p. 149 – Add the following at the end of footnote 43:

For a discussion of how “willpower norms” (norms that regulate temptation and willpower) can help us understand how to govern the disclosure of personal information, see Katherine J. Strandburg, Privacy, Rationality, and Temptation: A Theory of Willpower Norms, 57 Rutgers L. Rev. 1235 (2005).

2. DISCLOSURE OF ILLEGA LY OBTAINED INFORMATION

p. 159 – Add new note after note 3 to Bartnicki v. Vopper:

4. Interpreting the Scope of Bartnicki. In Boehner v. McDermott, 484 F.3d 573 (D.C. Cir. 2007), U.S. Representative James McDermott was provided a tape of a conference call between U.S. Representative John Boehner, then-Speaker of the House Newt Gingrich, and other Republican Party members. Boehner participated via a cell phone, and John and Alice Martin intercepted the call with a police radio scanner. They gave the tape to another member of the U.S. House, and the tape was eventually forwarded on to McDermott, the ranking Democrat on the Ethics Committee. Along with the tape was a letter from the Martins stating that the call was “heard over a scanner” and that they understood that they would be granted immunity. McDermott contacted reporters at the Atlanta Journal-Constitution and The New York Times. He played the tape to the New York Times reporter, who wrote a story about the tape. The Martins were prosecuted for a violation of the Wiretap Act, 18 U.S.C. § 2511(1)(a), prohibiting the interception of wire, oral, or electronic communications. They pled guilty and paid a $500 fine.

Boehner sued McDermott for violating 18 U.S.C. § 2511(1)(c), which prohibits disclosing a communication that one knows or has reason to know is acquired in violation of the Wiretap Act. The D.C. Circuit, en banc, concluded that Bartnicki could be distinguished:

Whatever the Bartnicki majority meant by “lawfully obtain,” the decision does not stand for the proposition that anyone who has lawfully obtained truthful information of public importance has a First Amendment right to disclose that information. Bartnicki avoided laying down such a broad rule of law, and for good reason. There are many federal provisions that forbid individuals from disclosing information they have lawfully obtained. The validity of these provisions has long been assumed. Grand jurors, court reporters, and prosecutors, for instance, may “not disclose a matter occurring before the grand jury.” Fed. R. Crim. P. 6(e)(2)(B). The Privacy Act imposes criminal penalties on government employees who disclose agency records containing information about identifiable individuals to unauthorized persons. See 5 U.S.C. § 552a(i)(1). The Espionage Act punishes officials who willfully disclose sensitive national defense information to persons not entitled to receive it. See 18 U.S.C. § 793(d). The Intelligence Identities Protection Act prohibits the disclosure of a covert intelligence agent’s identity. See 50 U.S.C. § 421. Employees of the Internal Revenue Service, among others, may not disclose tax return information. See 26 U.S.C. § 6103(a). State motor vehicle department employees may not make public information about an individual’s driver’s license or registration. See 18 U.S.C. § 2721. Employees of the Social Security Administration, as well as other government employees, may not reveal social security numbers or records. See 42 U.S.C. § 405(c)(2)(C)(viii)(I), (III). Judicial employees may not reveal confidential information received in the course of their official duties. See Code of Conduct for Judicial Employees Canon 3D. And so forth.

In analogous contexts the Supreme Court has sustained restrictions on disclosure of information even though the information was lawfully obtained. The First Amendment did not shield a television station from liability under the common law right of publicity when it filmed a plaintiff’s “human cannonball” act and broadcast the film without his permission. Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562 (1977). When a newspaper divulged the identity of an individual who provided information to it under a promise of confidentiality, the First Amendment did not provide the paper with a defense to a breach of contract claim. Cohen v. Cowles Media Co., 501 U.S. 663 (1991). The First Amendment did not prevent the government from enforcing reasonable confidentiality restrictions on former employees of the CIA. See Snepp v. United States, 444 U.S. 507 (1980). Parties to civil litigation did not “have a First Amendment right to disseminate, in advance of trial, information gained through the pretrial discovery process.” Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984).

In United States v. Aguilar, 515 U.S. 593 (1995), a case closely analogous to this one, the Supreme Court held that the First Amendment did not give a federal judge, who obtained information about an investigative wiretap from another judge, the right to disclose that information to the subject of the wiretap. The judge challenged his conviction for violating 18 U.S.C. § 2232(c), which prohibits the improper disclosure of an investigative wiretap. In rejecting his First Amendment claim, the Court wrote that the judge was not “simply a member of the general public who happened to lawfully acquire possession of information about the wiretap; he was a Federal District Court Judge who learned of a confidential wiretap application from the judge who had authorized the interception, and who wished to preserve the integrity of the court. Government officials in sensitive confidential positions may have special duties of non-disclosure.”

Aguilar stands for the principle that those who accept positions of trust involving a duty not to disclose information they lawfully acquire while performing their responsibilities have no First Amendment right to disclose that information. The question thus becomes whether, in the words of Aguilar, Representative McDermott’s position on the Ethics Committee imposed a “special” duty on him not to disclose this tape in these circumstances. Bartnicki has little to say about that issue. The individuals who disclosed the tape in that case were private citizens who did not occupy positions of trust.
All members of the Ethics Committee, including Representative McDermott, were subject to Committee Rule 9, which stated that “Committee members and staff shall not disclose any evidence relating to an investigation to any person or organization outside the Committee unless authorized by the Committee.”

There is no question that the rules themselves are reasonable and raise no First Amendment concerns.

If the First Amendment does not protect Representative McDermott from House disciplinary proceedings, it is hard to see why it should protect him from liability in this civil suit. Either he had a First Amendment right to disclose the tape to the media or he did not. If he had the right, neither the House nor the courts could impose sanctions on him for exercising it. If he did not have the right, he has no shield from civil liability or from discipline imposed by the House. In that event, his civil liability would rest not on his breach of some ethical duty, but on his violation of a federal statute for which he had no First Amendment defense. The situation is the same as that in Aguilar. There the defendant-judge was punished not for violating his ethical duty to maintain judicial secrecy, but for violating the general prohibition on disclosing investigative searches.

When Representative McDermott became a member of the Ethics Committee, he voluntarily accepted a duty of confidentiality that covered his receipt and handling of the Martins’ illegal recording. He therefore had no First Amendment right to disclose the tape to the media.

Judge Sentelle, along with several others, dissented:

There is no distinction of legal, let alone constitutional, significance between our facts and those before the Court in Bartnicki.

The Supreme Court has decided the first issue of this case, that is, whether the United States (or Florida) can constitutionally bar the publication of information originally obtained by unlawful interception but otherwise lawfully received by the communicator, in the negative. We venture to say that an opposite rule would be fraught with danger. Just as Representative McDermott knew that the information had been unlawfully intercepted, so did the newspapers to whom he passed the information. Representative Boehner has suggested no distinction between the constitutionality of regulating communication of the contents of the tape by McDermott or by The Washington Post or The New York Times or any other media resource. For that matter, every reader of the information in the newspapers also learned that it had been obtained by unlawful intercept. Under the rule proposed by Representative Boehner, no one in the United States could communicate on this topic of public interest because of the defect in the chain of title. We do not believe the First Amendment permits this interdiction of public information either at the stage of the newspaper-reading public, of the newspaper-publishing communicators, or at the stage of Representative McDermott’s disclosure to the news media. Lest someone draw a distinction between the First Amendment rights of the press and the First Amendment speech rights of nonprofessional communicators, we would note that one of the communicators in Bartnicki was himself a news commentator, and the Supreme Court placed no reliance on that fact.
C. DISSEMINATION OF FALSE OR MISLEADING INFORMATION
1. DEFAMATION

(b) Defamation and the Internet

p. 168 – Add the following at the end of note 1:

In *Barnes v. Yahoo!, Inc.*, 2005 WL 3005602 (D. Or. 2005), a woman alleged that her former boyfriend created fake profiles under her name on Yahoo. He posted nude photos of her in the profiles and provided contact information for her. She also claimed that he was impersonating her in chatrooms and directing people to the profiles. She contacted Yahoo and asked them several times to try to put a stop to the boyfriend’s misuse of Yahoo’s services. She alleged that although Yahoo employees promised they would help her, they failed to stop the boyfriend’s conduct. The court, in an unpublished opinion, concluded that Yahoo was immune under §230.

p. 169 – Add the following to the end of note 3:

The California Supreme Court reversed the court of appeals in *Barrett v. Rosenthal*, 146 P.3d 510 (Cal. 2006):

We agree with the *Zeran* court, and others considering the question, that subjecting Internet service providers and users to defamation liability would tend to chill online speech.

We reject the argument that the difficulty of prevailing on a defamation claim mitigates the deterrent effect of potential liability. Defamation law is complex, requiring consideration of multiple factors. These include whether the statement at issue is true or false, factual or figurative, privileged or unprivileged, whether the matter is of public or private concern, and whether the plaintiff is a public or private figure. Any investigation of a potentially defamatory Internet posting is thus a daunting and expensive challenge. For that reason, we have observed that even when a defamation claim is “clearly nonmeritorious,” the threat of liability “ultimately chills the free exercise of expression.”

Nor are we convinced by the observation that a “distributor” faces no liability without notice. Distributors are liable not merely upon receiving notice from a third party, but also if they independently “knew or had reason to know” of the defamatory statement. Thus, as the *Zeran* court pointed out, this aspect of distributor liability would discourage active monitoring of Internet postings. It could also motivate providers to insulate themselves from receiving complaints. Such responses would frustrate the goal of self-regulation.

The third practical implication noted in *Zeran* is no less compelling, and went unaddressed by the Court of Appeal. Notice-based liability for service providers would allow complaining parties to impose substantial burdens on the freedom of Internet speech by lodging complaints whenever they were displeased by an online posting.

Requiring providers, users, and courts to account for the nuances of common law defamation, and all the various ways they might play out in the Internet environment, is a Herculean assignment that we are reluctant to impose. We conclude the *Zeran* court accurately diagnosed the problems that would attend notice-based liability for service providers.

p. 169 – Add new note after note 3:

4. *Who Is the Content Provider?* In *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003), a handyman (Robert Smith) who worked at Ellen Batzel’s home emailed Ton Cremers, the director of security at a museum in Amsterdam, who maintained an email listserv about looted art. Smith said that several of Batzel’s paintings were stolen from the
Jews by the Nazis during World War II. Cremers made a few small changes to the text of Smith’s email and sent it out to his listerv. The paintings were not looted art from the Nazis, and Batzel sued both Smith and Cremers. The court concluded that since Cremers was not the originator of the information, he was immune under §230:

> Obviously, Cremers did not create Smith’s e-mail. Smith composed the e-mail entirely on his own. . . . [T]he exclusion of “publisher” liability necessarily precludes liability for exercising the usual prerogative of publishers to choose among proffered material and to edit the material published while retaining its basic form and message.

> Because Cremers did no more than select and make minor alterations to Smith’s e-mail, Cremers cannot be considered the content provider of Smith’s e-mail for purposes of § 230. . . .

> We therefore hold that a service provider or user is immune from liability under § 230(c)(1) when a third person or entity that created or developed the information in question furnished it to the provider or user under circumstances in which a reasonable person in the position of the service provider or user would conclude that the information was provided for publication on the Internet or other “interactive computer service.”

In dissent, Judge Gould wrote:

> Under my interpretation of § 230, a company that operates an e-mail network would be immune from libel suits arising out of e-mail messages transmitted automatically across its network. Similarly, the owner, operator, organizer, or moderator of an Internet bulletin board, chat room, or listerv would be immune from libel suits arising out of messages distributed using that technology, provided that the person does not actively select particular messages for publication.

> On the other hand, a person who receives a libelous communication and makes the decision to disseminate that messages to others—whether via e-mail, a bulletin board, a chat room, or a listerv—would not be immune. . . .

> Congress wanted to ensure that excessive government regulation did not slow America’s expansion into the exciting new frontier of the Internet. But Congress did not want this new frontier to be like the Old West: a lawless zone governed by retribution and mob justice. The CDA does not license anarchy. A person’s decision to disseminate the rankest rumor or most blatant falsehood should not escape legal redress merely because the person chose to disseminate it through the Internet rather than through some other medium. . . .

> In this case, I would hold that Cremers is not entitled to CDA immunity because Cremers actively selected Smith’s e-mail message for publication.

_Batzel_ demonstrates the difficulties in certain situations of determining whether a person is providing content or is merely disseminating the content of another. If a person is deemed the content provider, then §230 immunity does not apply, as §230 is designed to immunize a person from being liable for disseminating the content of others. In _Batzel_, is Cremers the content provider since he decided to forward the email? Or is Smith the content provider because he wrote the email? _Batzel_ holds that if a person receives a communication sent by another for the purpose of having the person publish it online, then the person is immune under §230 for publishing it. Few courts have adopted a rule like that in _Batzel_ because few have explored situations where it is unclear who precisely is the content provider.

Suppose Cremers has a blog about stolen art. Smith is interested in spreading the rumor about the stolen art on Cremers’ blog. Consider the following situations and examine whether Cremers would have §230 immunity under the majority’s rule and also under Judge Gould’s.
(a) Cremers’ blog allows anybody to post comments. Smith posts a comment about the rumor on Cremers’ blog. Batzel wants Cremers to delete the comment, but Cremers refuses to do so.

(b) Cremers has a comment moderation system on his blog where he must approve comments before they are published on his blog. Smith posts the stolen art comment and Cremers approves it, whereupon it is published on the blog.

(c) Smith emails Cremers and tells him about the stolen art rumor. Instead of posting the email itself, Cremers writes a blog post about the rumor in his own words and posts it.

(d) Smith calls Cremers and tells him the rumor about the stolen art. Cremers writes a post about the rumor.

Is there any meaningful difference between the above situations and the way that Cremers disseminated Smith’s email to the listserv? As a normative matter, should Cremers’ liability be different in any of the above situations? How should the law determine when a person should be deemed the content provider and when a person should be deemed to merely be relaying the content of another?

5. Wikipedia. Wikipedia is an online encyclopedia that anybody can edit. It has millions of entries and is widely used and cited. What are the legal consequences when a Wikipedia entry is defamatory?

A notable case occurred in 2005 involving John Seigenthaler, a former assistant to Attorney General Bobby Kennedy during the Kennedy Administration. His Wikipedia entry falsely accused him of being involved in President John F. Kennedy’s assassination. In an article in USA Today, Seigenthaler wrote:

I have no idea whose sick mind conceived the false, malicious “biography” that appeared under my name for 132 days on Wikipedia, the popular, online, free encyclopedia whose authors are unknown and virtually untraceable.5

Eventually, the anonymous person who wrote the defamatory statement was identified, and he apologized. If Seigenthaler sued Wikipedia for defamation, would § 230 provide Wikipedia with immunity? Consider the views of Ken Myers on this topic:

Because of the unique relationship between Wikipedia and its user-community, the question of whether an individual user-poster is a separate “information content provider,” as opposed to somehow being a representative of Wikipedia, is unclear. If Wikipedia is determined to be the relevant “information content provider” then there is no immunity under § 230(c)(1), as Wikipedia itself will be held responsible for the defamatory content. Thus, the definition of “information content provider” raises an important threshold question in this case: what counts as the “person or entity” whose actions the court should analyze in determining whether Wikipedia is the “information content provider” under the third prong? . . . .

The Wikipedia community is self-consciously inclusive, designating all of its contributors as “Wikipedians.” Presumably, this inclusiveness fosters the cooperative atmosphere critical to Wikipedia’s success. However, if all members of the Wikipedia community - that is, all contributors - are considered part of the Wikipedia “entity,” then it would, by definition and by operation of the third prong, not be eligible for § 230(c)(1) immunity because Wikipedia would be the site’s only contributor - there could be no “[other information content provider.” Wikipedia’s self-perception notwithstanding, that particular result does not seem likely in light of

the courts’ treatment of other community-based “interactive computer services.” For example, in the case of the dating site matchmaker.com, the court assumed that the user “contributing” the content (a defamatory profile) served as the “[other information content provider” for purposes of the third prong and thus was not part of the matchmaker.com “entity.” A different court made the same assumption and reached the same result more recently in a similar situation, where a user (the plaintiff’s ex-boyfriend) created a false Yahoo! profile with nude pictures of the plaintiff.

Wikipedia is similar to matchmaker.com in that a community of users creates the content that gives purpose to the community. Wikipedia is also similar to Yahoo! in that anyone can join and create content purely for the sake of sharing it with others. The difference lies in the formal organizational structure. Wikipedia lacks the sharp demarcation that, in the cases of matchmaker.com and Yahoo!, separates the profile-contributors from the sites’ governing powers.

Most significantly, at the sysop level, the user gains the power to edit “protected” pages, including the pages that mandate Wikipedia’s legal policies. This power to alter Wikipedia’s legal policies reflects the Restatement’s definition of agency, which notes that “[w]hen an agent acts with actual authority, the agent’s power to affect the principal’s legal relations with third parties is coextensive with the agent’s right to do so, which actual authority creates.” Wikipedians with sysop powers are thus more analogous to matchmaker.com and Yahoo! employees, who run the matchmaker.com and Yahoo! Profile services, than to the users who merely contribute profiles to those services.

Wikipedia would argue that, for purposes of § 230(f)(3), only employees of the Wikimedia Foundation should be considered as part of the Wikipedia “entity.” However, “the fact that work is performed gratuitously does not relieve a principal of liability.”

Myers ultimately concludes that Wikipedia would probably not be liable if the defamatory statement was submitted by a regular user. But to the extent that websites like Wikipedia create hierarchies of users, with some having greater editorial powers like sysops, does this alter immunity for the actions of the users at the top of the hierarchy?

6. Is § 230 Immunity Too Broad? Consider Daniel Solove:

In one case, a woman’s ex-boyfriend impersonated her in a Yahoo! chat room. Anybody can sign up as a Yahoo! user for free and can use any name. The ex-boyfriend posted naked photos of the woman and included her email address and work phone number. His goal was to get men to start harassing her. When she discovered what happened, the woman was appalled. According to the woman, she wrote to Yahoo!, explaining that she didn’t create this profile and wanted the photos removed. A month passed, and Yahoo! did nothing. She wrote to Yahoo! again. No response. Finally, she spoke with a Yahoo! employee, who promised to help her remove the photos. But the woman claims that Yahoo! still didn’t get the photos taken down.

The woman sued Yahoo! but the court threw out the case because Yahoo! was immune under Section 230. If Yahoo! or bloggers can be liable if, after being informed, they fail to remove a comment that is defamatory or invasive of privacy, then they might become too cautious and remove comments too quickly. This will have a negative impact on speech, because if a person doesn’t like a comment about herself, ISPs or bloggers might be extra careful and remove it in order to avoid a lawsuit. The result would be a kind of heckler’s veto, where a person could have a comment removed by complaining about it, whether justifiably or not.

On the other hand, if Yahoo! or bloggers ignore a person’s complaints about harmful comments, then that person might be without much recourse. Shouldn’t Yahoo! have removed the photos? This seems like an awful situation for the plaintiff—nude photos of herself, as well as her contact information, are placed on the Internet and she is helpless in getting them removed. Is there such a big harm in forcing Yahoo! to remove them? Shouldn’t people have some ability to halt the distribution of nude pictures or falsehoods or other personal information about themselves?

---

on the Internet? While the plaintiff shouldn’t be entitled to obtain large money damages from Yahoo! the law should provide an incentive for Yahoo! to respond to legitimate take-down requests. Copyright law, for example, provides for a such a system when users of Internet service providers like Yahoo! post content that infringes upon copyright. Internet services providers are not liable if they remove copyright-infringing content posted by their users. Notice and take-down systems down can certainly be abused by people requesting removal of content that is not defamatory or invasive of privacy, but the law could address this problem by penalizing abusers.\(^7\)

Is a notice and take-down system preferable to a broader immunity that eliminates distributor liability entirely? Is it feasible to punish abusers of a notice and take-down system?

**D. APPROPRIATION OF NAME OR LIKENESS**

p. 197 – Insert new subsection 3. FOR ONE’S OWN USE OR BENEFIT. Renumber existing subsection 3 to subsection 4.

3. FOR ONE’S OWN USE OR BENEFIT

The Restatement of Torts recognizes appropriation of another’s name or likeness when it is used for the appropriator’s “own use or benefit.” What does “use or benefit” mean? In many jurisdictions, appropriation occurs only when the use or benefit is commercial in nature – i.e., used to promote or endorse a service or product.

**RAYMEN v. UNITED SENIOR ASSOCIATION, INC.**


WALTON, J. On March 9, 2005, the plaintiffs filed this action seeking to prevent the defendants from further using their images in an advertising campaign which challenged various public policy positions taken by the American Association of Retired Persons (“AARP”) regarding Social Security reform and the military. Currently before the Court are the defendants’ motions to dismiss, and the plaintiffs’ opposition thereto.

On March 3, 2004, the plaintiffs were among 300 citizens of Multnomah County, Oregon who were married pursuant to a newly established right to same-sex marriage in that county. While at City Hall awaiting their opportunity to marry, the plaintiffs, Steve Hansen and Richard Raymen, kissed. A photographer from a Portland, Oregon newspaper, the Tribune, captured the kiss in a photograph he took. The photograph was subsequently published in both the Tribune newspaper on March 4, 2004, and later on the Tribune’s website. At some later point in time, the Tribune’s website photograph was used without permission as part of an advertisement created by defendant Mark Montini. The advertising campaign was created for a nonprofit organization, United Senior Association, Inc., which does business under the name USA Next. The advertisement, which features the photograph of the plaintiffs kissing, was part of a campaign by USA Next challenging various public policy positions purportedly taken by the AARP. Specifically, the advertisement contains two pictures. The first is a picture of an

American soldier, who presumably is in Iraq, with a red “X” superimposed over it, and the second is the photograph of the plaintiffs with a green checkmark superimposed over it. The caption under the advertisement reads: “The Real AARP Agenda,” suggesting that the AARP opposes the United States military efforts abroad and supports the gay lifestyle. This advertisement ran on the website of The American Spectator magazine from February 15, 2005, to February 21, 2005.

According to the plaintiffs, the purpose of the advertising campaign was “to incite viewer passions against the AARP because of its alleged support of equal marriage rights for same-sex couples and its alleged lack of support of American troops.” Moreover, the plaintiffs opine that the “advertisement also conveys the message that the plaintiffs ... are against American troops ... and are unpatriotic.” The plaintiffs contend that the advertisement attracted media attention, which then caused an even wider distribution of the advertisement throughout the media. The plaintiffs assert that because of the advertisement, they “have suffered embarrassment, extreme emotional distress, and the invasion of their privacy.” In addition, the plaintiffs represent that as a result of the false and misleading inference “communicated by the [a]dvertisement about [the] plaintiffs, their reputations as patriotic American citizens has been severely damaged.” . . .

“One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.” Martinez v. Democrat-Herald Publ’g Co., Inc., 669 P.2d 818, 820 (1983) (quoting Restatement (Second) of Torts § 652C (1976)). Under § 652C of the Restatement, plaintiffs can recover “damages when their names, pictures or other likenesses have been used without their consent to advertise a defendant’s product, to accompany an article sold, to add luster to the name of a corporation or for some other business purpose.” However, there is no actionable appropriation of a person’s likeness claim “when a person’s picture is used to illustrate a noncommercial, newsworthy article.” . . . Whether a communication is commercial or noncommercial is a question of law. . . .

The photograph of the plaintiffs was used as part of USA Next’s advertising campaign, which sought, at least in part, to engender opposition to AARP’s policy position on social security reform. Presumably, the advertisement sought to vilify the AARP by conveying a message concerning AARP’s alleged views on two hot button policy issues-support of same-sex marriage and opposition to the military. While the advertisement itself lacked any substantive discussion of these issues, it did convey AARP’s purported position on both subjects. And someone who viewed the advertisement online could then access the USA Next’s webpages which described the organization and its position on Social Security reform. Clearly the issues of same-sex marriage and support for the military are issues of public concern and both have been widely discussed in the media. In fact, the plaintiffs contend in their complaint that the purpose of the advertisement was to influence Congress.

The plaintiffs’ argument that the advertisement is commercial in nature because it sought contributions and promoted USA Next’s lobbying services, is unpersuasive. First, nothing in the advertisement itself seeks donations. Rather, only after using the advertisement (by clicking on it) to access the webpages were viewers exposed to the information about USA Next and the solicitation for financial contributions. This Court cannot conclude that this detached solicitation elevates the advertisement itself to a level where it can be deemed commercial in nature. See, e.g., Martinez, 669 P.2d at 820 (“The
fact that the defendant is engaged in the business of publication, for example of a newspaper, out of which he makes or seeks to make a profit, is not enough to make the incidental publication of a commercial use of the name or likeness.”) (quoting Restatement (Second) Torts § 652C, cmt. D (1976)). Moreover, contrary to the plaintiffs’ assertion, this case is not analogous to . . . Beverley v. Choices Women’s Med. Ctr. Inc., 587 N.E.2d 275 (N.Y. 1991). . . .

In Beverley, the Court concluded that a calendar produced by a for-profit hospital was commercial in nature because it had the hospital’s “name, logo, address, and telephone number on each page of the calendar,” along with “glowing characterizations and endorsements concerning the services” provided by the hospital, and thus left no doubt that the calendar was created to preserve existing patronage and to solicit new patients. Here, the advertisement does not even associate itself with USA Next through the use of its address, telephone number, logo, or in any other manner. Moreover, the calendar in Beverley promoted the use of the hospital’s services, while the advertisement here discusses public policy issues that are currently the subject of public debate. . . .

NOTES & QUESTIONS

1. The Fuzzy Line Between Commercial and Non-Commercial Uses. Is using a person’s photograph to solicit donations a commercial use? In Raymen, the image of the plaintiffs kissing was used not as a positive endorsement but as a way to spark outrage in their readers and spur them to donate. Isn’t this using their image for financial gain? On the other hand, the plaintiffs’ anger at the use of their photograph stems from their outrage over the defendants’ message. The defendant could argue that the image of the plaintiffs was a popular iconic image representing gay marriage. Should the plaintiffs be able to control that image whenever they dislike the viewpoints of those that use it?

2. Girls Gone Wild. Consider the case of Lane v. MRA Holdings, LLC, 242 F. Supp. 2d 1205 (M.D. Fla. 2002). The plaintiff was approached by a crew who produced the Girls Gone Wild video series, a set of videos showing women stripping at various parties and events, such as spring break or Marti Gras. The plaintiff claimed that the crew promised that the footage would be for their personal use only, but it was used in a Girls Gone Wild video. Among many claims, the plaintiff argued that the makers of Girls Gone Wild appropriated her likeness. The court, however, rejected her appropriation claim:

The Defendants first argue that they are not liable under Fla. Stat. § 540.08 because they did not use Lane’s image for trade, commercial, or advertising purposes. Under Fla. Stat. § 540.08, the terms “trade”, “commercial”, or “advertising purpose” mean using a person’s name or likeness to directly promote a product or service.

As a matter of law, this Court finds that Lane’s image and likeness were not used to directly promote a product or service. In coming to this conclusion, this Court relies upon Section 47 of the Restatement (Third) of Unfair Competition which defines “the purposes of trade” as follows:

The names, likeness, and other indicia of a person’s identity are used “for the purposes of trade” ... if they are used in advertising the user’s goods or services, or are placed on merchandise marketed by the user, or are used in connection with services rendered by the user. However, use “for the purpose of trade” does not ordinarily include the use of a
person’s identity in news reporting, commentary, entertainment, works of fiction or nonfiction, or in advertising incidental to such uses.

Therefore, under this definition, the “use of another’s identity in a novel, play, or motion picture is ...not ordinarily an infringement ... [unless] the name or likeness is used solely to attract attention to a work that is not related to the identified person...”  Id. at comment c.

In this case, it is irrefutable that the Girls Gone Wild video is an expressive work created solely for entertainment purposes. Similarly, it is also irrefutable that while Lane’s image and likeness were used to sell copies of Girls Gone Wild, her image and likeness were never associated with a product or service unrelated to that work. Indeed, in both the video and its commercial advertisements, Lane is never shown endorsing or promoting a product, but rather, as part of an expressive work in which she voluntarily participated. Consequently, in accordance with Section 47 of the Restatement, the use of Lane’s image or likeness in Girls Gone Wild, and in the marketing of that video cannot give rise to liability.

Upon reviewing Florida case law, it has come to this Court’s attention that only one case has applied the provisions of Fla. Stat. § 540.08 to an expressive work. In Gritzke v. M.R.A. Holding, LLC, No. 4:01cv495-RH (N.D. Fla. Mar., 15, 2002), Judge Hinkle of the Northern District of Florida determined that the plaintiff stated a valid claim under § 540.08 by alleging that her half naked image was plastered on the front cover of the videotape Girls Gone Wild without her authorization.

[T]he plaintiff in Gritzke was complaining about the use of her image on the outside cover of a videotape package. In this case, Lane has not alleged that her image was plastered on a billboard or box cover advertising Girls Gone Wild. Rather, this cause of action arises from the Defendants truthful and accurate depiction of Lane voluntarily exposing her breasts to a camera, just as she did on Labor Day Weekend in Panama City Beach, Florida. Unlike in Gritzke, the Plaintiff’s image in this case was never doctored. It has always remained in its original video format. Accordingly, the Gritzke case offers Lane little assistance.

Lane’s lawsuit arose from an expressive work that has no purpose other than to entertain a segment of the general population. [T]he Plaintiff in this case is not shown endorsing or promoting a product, but rather as participating in an expressive work. [T]his Court finds that the publication of Girls Gone Wild is not actionable simply because it is sold for a profit.
CHAPTER 3:
PRIVACY AND LAW ENFORCEMENT

SUMMARY OF ADDITIONS TO CHAPTER

• In A.1(g) (checkpoints), we added a discussion of MacWade v. Kelly, a case involving a random search program in the New York City subway system.

• In B.4 (CALEA), we updated the material on VoIP to reflect important new FCC activity.

• In B.5 (FISA), we added an excerpt from United States  v. United States District Court (Keith) (1972), the leading Supreme Court case regarding FISA.

• In C (Intelligence, Terrorism, and National Security), we added a new section with updated information about the NSA Surveillance program and excerpts from the Protect America Act from August 2007, which amended FISA.

• In E (government computer searches), we added a new section pertaining to shared computers and password protection, along with an excerpt from United States v. Andrus.

• in E.3, we added a new section regarding email and a new case, Warshak v. U.S.

A. THE FOURTH AMENDMENT AND EMERGING TECHNOLOGY
1. INTRODUCTION
(g) Checkpoints

p. 212 – Add the following at the end of the section on checkpoints:

In MacWade v. Kelly, 460 F.3d 260 (2d Cir. 2006), the New York Police Department instituted a random search program in the subways following a bombing on a subway in London. Police searched people’s bags and other items as they entered the station. Those wishing not to be searched could leave the station. The court upheld the program under a Fourth Amendment challenge:

Given the subway’s enclosed spaces, extraordinary passenger volume, and cultural and economic importance, it is unsurprising--and undisputed--that terrorists view it as a prime target. In fact, terrorists have targeted it before. In 1997, police uncovered a plot to bomb Brooklyn’s Atlantic Avenue subway station--a massive commuter hub that joins 10 different subway lines and the Long Island Railroad. In 2004, police thwarted another plot to bomb the Herald Square subway station, which networks eight different subway lines in midtown Manhattan. . . .

The NYPD designed the Program chiefly to deter terrorists from carrying concealed explosives onto the subway system and, to a lesser extent, to uncover any such attempt. Pursuant
to the Program, the NYPD establishes daily inspection checkpoints at selected subway facilities. A “checkpoint” consists of a group of uniformed police officers standing at a folding table near the row of turnstiles disgorging onto the train platform. At the table, officers search the bags of a portion of subway riders entering the station.

In order to enhance the Program’s deterrent effect, the NYPD selects the checkpoint locations “in a deliberative manner that may appear random, undefined, and unpredictable.” In addition to switching checkpoint locations, the NYPD also varies their number, staffing, and scheduling so that the “deployment patterns ... are constantly shifting.” While striving to maintain the veneer of random deployment, the NYPD bases its decisions on a sophisticated host of criteria, such as fluctuations in passenger volume and threat level, overlapping coverage provided by its other counter-terrorism initiatives, and available manpower.

Although a subway rider enjoys a full privacy expectation in the contents of his baggage, the kind of search at issue here minimally intrudes upon that interest. Several uncontested facts establish that the Program is narrowly tailored to achieve its purpose: (1) passengers receive notice of the searches and may decline to be searched so long as they leave the subway; (2) police search only those containers capable of concealing explosives, inspect eligible containers only to determine whether they contain explosives, inspect the containers visually unless it is necessary to manipulate their contents, and do not read printed or written material or request personal information; (3) a typical search lasts only for a matter of seconds; (4) uniformed personnel conduct the searches out in the open, which reduces the fear and stigma that removal to a hidden area can cause; and (5) police exercise no discretion in selecting whom to search, but rather employ a formula that ensures they do not arbitrarily exercise their authority.

[W]e need only determine whether the Program is “a reasonably effective means of addressing” the government interest in deterring and detecting a terrorist attack on the subway system.

We will not peruse, parse, or extrapolate four months’ worth of data in an attempt to divine how many checkpoints the City ought to deploy in the exercise of its day-to-day police power. Counter-terrorism experts and politically accountable officials have undertaken the delicate and esoteric task of deciding how best to marshal their available resources in light of the conditions prevailing on any given day. We will not--and may not--second-guess the minutiae of their considered decisions.

Instead, we must consider the Program at the level of its design. . . . From that vantage, the expert testimony established that terrorists seek predictable and vulnerable targets, and the Program generates uncertainty that frustrates that goal, which, in turn, deters an attack.

Is the New York City program of subway searches an effective measure as the Second Circuit suggests? According to the court’s opinion, just how effective or useful does such a search have to be?

In a forthcoming article, Daniel Solove faults the MacWade court for not assessing the statistical data available about the program effectiveness. Solove writes, “The way the court analyzed the government’s side of the balance would justify nearly any search, no matter how ineffective. Although courts should not take a know-it-all attitude, they must not defer on such a critical question as a security measure’s effectiveness.” In Solove’s judgment:

A very small number of random searches in a subway system of over four million riders a day seems more symbolic than effective, because the odds of the police finding the terrorist with a bomb are very low. The government also argued that the program would deter terrorists from bringing bombs on subway trains, but nearly any kind of security measure can arguably produce some degree of deterrence. The key issue, which the court did not analyze, is whether it would be a significant amount of deterrence to outweigh the curtailment in civil liberties.8

Do you agree with this critique? Will the subway searches create “a significant amount of deterrence”? What is the curtailment of civil liberties created by the New York subway searches, and how great is it in your view?

Bruce Schneier has developed an important concept that he terms “security theater.” According to Schneier, security theater is action that seeks to increase our feeling of security without actually making us safer.9 As an example, a requirement to show an ID before entering an office building, a common obligation in New York City, does nothing to increase our security against terrorists. The problem with security theater is that it wastes resources and prevents investment in policies that would protect us by fooling us into thinking that we are safe.

Yet, Schneier has also argued that security theater can sometimes have a positive impact: “It’s only a waste if you consider the reality of security exclusively. There are times when people feel less secure than they actually are. In those cases, … a palliative countermeasure that primarily increases the feeling of security is just what the doctor ordered.”10 The bottom line? Schneier want us to evaluate whether politicians, corporations, or others are “using security theater to make us feel more secure without doing the hard work of actually making us secure.”

Do you think the New York City program of subway searches is best understood as “security theater”? If so, do you think it is a positive or negative example of this phenomenon.

p. 238 – Add the following at the end of note 4:

In an analysis of state constitutional law, Stephen Henderson concludes that eleven states have rejected the third party doctrine: California, Florida, Idaho, Montana, Pennsylvania, Washington, Colorado, Hawaii, Illinois, New Jersey, and Utah. Ten more states have not explicitly rejected the third party doctrine, but have caselaw suggesting that they might do so in the future.11

p. 238 – Add the following after note 4:

5. The First Amendment and Pen Register Information. Daniel Solove argues that the First Amendment should be understood as a source of criminal procedure and should protect pen register information:

Although the Supreme Court has focused on the Fourth Amendment, obtaining pen register data without a warrant potentially violates the First Amendment. A log of incoming and outgoing calls can be used to trace channels of communication. It is relatively easy to link a phone number to a person or organization. Pen registers can reveal associational ties, since association in contemporary times often occurs by way of telephone or e-mail. As David Cole argues, modern communications technology has made association possible without physical assembly. For example, if the government scrutinized the phone logs of the main office of the Communist Party, it might discover many of the Party’s members. The information would not be equivalent to a membership list, but it

---

9 Bruce Schneier, Beyond Fear 38 (2003).
would probably include identifying data about countless individuals who would not want the government to discover their connection to the Communist Party. If the government were to examine the phone logs or e-mail headers of a particular individual, it might discover that the individual contacted particular organizations that the individual wants to keep private. The pen register information, therefore, implicates First Amendment values.12

B. FEDERAL ELECTRONIC SURVEILLANCE LAW
4. THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT

p. 288 – Insert new material at end of material on VOIP:

The Federal Communications Commission continued its work in this area by issuing an Order in 2005 that built on its previous Notice of Proposed Rulemaking. This rulemaking, upheld by the D.C. Circuit in June 2006, established that broadband and VoIP are “hybrid telecommunications-information services” that fall under CALEA to the extent that they qualify as “telecommunications carriers.” Communications Assistance for Law Enforcement and Broadband Access and Services, 20 F.C.C.R. 14989, at ¶ 18 (2005); American Council on Education v. FCC, 451 F.3d 266 (D.C. Cir. 2006).

In May 2006, the FCC issued an additional order to address remaining issues to achieve CALEA compliance. Second Report and Order and Memorandum Opinion and Order (Order), FCC 06-56 (May 12, 2006). The FCC’s overarching policy perspective concerned giving law enforcement agencies all the resources that CALEA authorizes to combat crime and support homeland security. As FCC Chairman Kevin J. Martin observed in a statement issued as part of the Order, “Enabling law enforcement to ensure our safety and security is of paramount importance.”

The Order set a May 14, 2007 compliance data for both facilities-based broadband Internet access and interconnected VoIP providers. It also permitted entities covered by CALEA to have the option of using Trusted Third Parties (TTPs) to help meet their CALEA obligations. The role of the TTPs would include processing requests for intercepts, conducting electronic surveillance, and delivering relevant information to law enforcement agencies. Finally, the Order found that carriers were responsible for the costs of CALEA development for “post-January 1, 1995 equipment and facilities.” The FCC explicitly declined to adopt a national surcharge to cover CALEA costs. The Order found that a national surcharge would not serve the public interest; it would increase the administrative burden placed on carriers and providing little incentive for cost minimization on their part.

These FCC decisions can extend to colleges and universities that run their own private networks. Generally, private telecommunication networks are not subject to CALEA. Yet, these networks are subject to CALEA to the extent that they are interconnected with a public network, whether the traditional public switching telecommunications network or the Internet. Specifically, the facilities that connect the private network to the public network must be CALEA compliant. One FCC Commissioner, Deborah Taylor Tate, has pointed to the use of TTP as possibly providing

a low cost means for educational institutions to meet CALEA’s requirements. In her statement, issued as part of the Order of May 2006, she quoted one TTP’s assertion that the cost per IP service subscriber, based on large scale implementation, could be as low as one cent per subscriber per month—or even less.

There also have been also been objections to the FCC’s decisions that find CALEA obligations for Internet and VoIP technologies. James Dempsey of the Center for Democracy and Technology testified before Congress in 2004 that the proof of the wisdom of Congress taking a “relatively non-regulatory approach to the Internet” has been demonstrated by the Internet's “rapid growth and innovation.” In contrast, “CALEA-type mandates would drive up costs, impair and delay innovation, threaten privacy, jeopardize Internet security, and force development of the latest Internet innovations offshore.” Dempsey proposed that instead of imposing the “centralized design mandates of CALEA” on VoIP, the government itself should simply “acquire the technology it needs to interpret Internet communications.”

Susan Landau and Whitford Diffie argue that extension of CALEA-requirements to the Internet will create an opening for terrorists to work havoc on the communications infrastructure of the U.S. Building surveillance capacity into the system will make it less secure and creates a potential for cyber-terrorism against the U.S. From Landau and Diffie’s perspective, “We should not take our strengths, which include modern and robust communication systems, and turn them into instruments of surveillance that others can use against us.” They write:

On balance we are better off with a secure computer infrastructure than with one that builds surveillance into the network fabric. At times this may press law enforcement to exercise more initiative and imagination in its investigations. On the other hand, in a society completely dependent on computer-to-computer communications, the alternative presents a hazard whose dimensions are as yet impossible to comprehend.

B. FEDERAL ELECTRONIC SURVEILLANCE LAW
5. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

UNITED STATES V. UNITED STATES DISTRICT COURT
THE “KEITH” CASE
407 U.S. 297 (1972)

POWELL, J. . . . The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President’s power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern, requiring sensitivity both to the Government’s right to protect itself from unlawful subversion and

14 Susan Landau & Whitford Diffie, Privacy on the Line 331, 328 (2d ed. 2007).
attack and to the citizen’s right to be secure in his privacy against unreasonable Government intrusion.

This case arises from a criminal proceeding in the United States District Court for the Eastern District of Michigan, in which the United States charged three defendants with conspiracy to destroy Government property. . . . One of the defendants, Plamondon, was charged with the dynamite bombing of an office of the Central Intelligence Agency in Ann Arbor, Michigan.

Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510-2520, authorizes the use of electronic surveillance for classes of crimes carefully specified in 18 U.S.C. § 2516. Such surveillance is subject to prior court order. Section 2518 sets forth the detailed and particularized application necessary to obtain such an order as well as carefully circumscribed conditions for its use. The Act represents a comprehensive attempt by Congress to promote more effective control of crime while protecting the privacy of individual thought and expression. Much of Title III was drawn to meet the constitutional requirements for electronic surveillance enunciated by this Court in Berger v. New York, and Katz v. United States.

The Government relies on § 2511(3). It argues that “in excepting national security surveillances from the Act’s warrant requirement Congress recognized the President’s authority to conduct such surveillances without prior judicial approval.” The section thus is viewed as a recognition or affirmation of a constitutional authority in the President to conduct warrantless domestic security surveillance such as that involved in this case.

We think the language of § 2511(3), as well as the legislative history of the statute, refutes this interpretation. The relevant language is that: “Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect . . .” against the dangers specified. At most, this is an implicit recognition that the President does have certain powers in the specified areas. Few would doubt this, as the section refers--among other things--to protection “against actual or potential attack or other hostile acts of a foreign power.” But so far as the use of the President’s electronic surveillance power is concerned, the language is essentially neutral.

Section 2511(3) certainly confers no power, as the language is wholly inappropriate for such a purpose. It merely provides that the Act shall not be interpreted to limit or disturb such power as the President may have under the Constitution. In short, Congress simply left presidential powers where it found them.

Our present inquiry, though important, is . . . a narrow one. It addresses a question left open by Katz:

Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security. . . .

We begin the inquiry by noting that the President of the United States has the fundamental duty, under Art. II, § 1, of the Constitution, to “preserve, protect and defend the Constitution of the United States.” Implicit in that duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means. In the discharge of this duty, the President--through the Attorney General--may find it necessary to employ electronic surveillance to obtain intelligence information on the plans of those
who plot unlawful acts against the Government. The use of such surveillance in internal security cases has been sanctioned more or less continuously by various Presidents and Attorneys General since July 1946.

Though the Government and respondents debate their seriousness and magnitude, threats and acts of sabotage against the Government exist in sufficient number to justify investigative powers with respect to them. 15 The covertness and complexity of potential unlawful conduct against the Government and the necessary dependency of many conspirators upon the telephone make electronic surveillance an effective investigatory instrument in certain circumstances. The marked acceleration in technological developments and sophistication in their use have resulted in new techniques for the planning, commission, and concealment of criminal activities. It would be contrary to the public interest for Government to deny to itself the prudent and lawful employment of those very techniques which are employed against the Government and its lawabiding citizens.

But a recognition of these elementary truths does not make the employment by Government of electronic surveillance a welcome development—even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens. We look to the Bill of Rights to safeguard this privacy. Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance. Our decision in Katz refused to lock the Fourth Amendment into instances of actual physical trespass.

. . . [N]ational security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of “ordinary” crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. . . . The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect “domestic security.” Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.

The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.

As the Fourth Amendment is not absolute in its terms, our task is to examine and balance the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression. If the legitimate need of Government to safeguard domestic security requires the use of electronic surveillance, the question is whether the needs of citizens for privacy and the free expression may not be better protected by requiring a warrant before such surveillance is undertaken. We must also

---

15 The Government asserts that there were 1,562 bombing incidents in the United States from January 1, 1971, to July 1, 1971, most of which involved Government related facilities. Respondents dispute these statistics as incorporating many frivolous incidents as well as bombings against nongovernmental facilities. The precise level of this activity, however, is not relevant to the disposition of this case.
ask whether a warrant requirement would unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it. . . .

[C]ontentions in behalf of a complete exemption from the warrant requirement, when urged on behalf of the President and the national security in its domestic implications, merit the most careful consideration. We certainly do not reject them lightly, especially at a time of worldwide ferment and when civil disorders in this country are more prevalent than in the less turbulent periods of our history. There is, no doubt, pragmatic force to the Government’s position.

[W]e do not think a case has been made for the requested departure from Fourth Amendment standards. The circumstances described do not justify complete exemption of domestic security surveillance from prior judicial scrutiny. Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President’s domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure.

We cannot accept the Government’s argument that internal security matters are too subtle and complex for judicial evaluation. Courts regularly deal with the most difficult issues of our society. There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases. . . . If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance.

Nor do we believe prior judicial approval will fracture the secrecy essential to official intelligence gathering. The investigation of criminal activity has long involved imparting sensitive information to judicial officers who have respected the confidentiality involved. Judges may be counted upon to be especially conscious of security requirements in national security cases. Title III of the Omnibus Crime Control and Safe Streets Act already has imposed this responsibility on the judiciary in connection with such crimes as espionage, sabotage, and treason, §§ 2516(1)(a) and (c), each of which may involve domestic as well as foreign security threats. Moreover, a warrant application involves no public or adversary proceedings: it is an ex parte request before a magistrate or judge. Whatever security dangers clerical and secretarial personnel may pose can be minimized by proper administrative measures, possibly to the point of allowing the Government itself to provide the necessary clerical assistance. . . .

We emphasize, before concluding this opinion, the scope of our decision. As stated at the outset, this case involves only the domestic aspects of national security. We have not addressed and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents. . . .

Moreover, we do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of “ordinary crime.” The gathering of security intelligence is often long
range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government’s preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.

Given those potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection. . . .

DOUGLAS J. CONCURRING. While I join in the opinion of the Court, I add these words in support of it. . . .

If the Warrant Clause were held inapplicable here, then the federal intelligence machine would literally enjoy unchecked discretion. Here, federal agents wish to rummage for months on end through every conversation, no matter how intimate or personal, carried over selected telephone lines, simply to seize those few utterances which may add to their sense of the pulse of a domestic underground. . . .

That “domestic security” is said to be involved here does not draw this case outside the mainstream of Fourth Amendment law. Rather, the recurring desire of reigning officials to employ dragnet techniques to intimidate their critics lies at the core of that prohibition. For it was such excesses as the use of general warrants and the writs of assistance that led to the ratification of the Fourth Amendment. . . .

[W]e are currently in the throes of another national seizure of paranoia, resembling the hysteria which surrounded the Alien and Sedition Acts, the Palmer Raids, and the McCarthy era. Those who register dissent or who petition their governments for redress are subjected to scrutiny by grand juries, by the FBI, or even by the military. Their associates are interrogated. Their homes are bugged and their telephones are wiretapped. They are befriended by secret government informers. Their patriotism and loyalty are questioned. . . .

We have as much or more to fear from the erosion of our sense of privacy and independence by the omnipresent electronic ear of the Government as we do from the likelihood that fomenters of domestic upheaval will modify our form of governing.

NOTES & QUESTIONS

1. Domestic Security versus Foreign Threats? The Keith Court draws a distinction among (1) electronic surveillance in criminal investigations, regulated under Title III; (2) electronic surveillance in domestic security investigations; and (3) electronic surveillance in investigations involving “activities of foreign powers and their agents.”

Regarding the first category, the Keith Court stated that there was no debate
regarding “the necessity of obtaining a warrant in the surveillance of crimes unrelated to the national security interest.” Regarding the second category, the focus of the Keith Court’s opinion, its holding was that the Fourth Amendment required the issuing of a warrant in domestic security investigations. It also held that the precise requirements for issuing a requirement to investigate domestic security need not be the same as for Title III criminal surveillance. Finally, it stated that it did not address issues involving foreign powers and their agents. Does this tripartite distinction seem useful as a policy matter?

2. The Three Keith Categories. Today, Title III and subsequent statutes, now codified in ECPA, regulate electronic surveillance in criminal investigations (category one above). The Foreign Intelligence Surveillance Act, as enacted in 1978, regulates electronic and other kinds of surveillance in cases involving foreign powers and their agents (category three).

What then of the Keith category of “domestic security investigations.” (category two)? Recall that the defendants in the underlying criminal proceeding were charged with a conspiracy to destroy government property. One of the defendants, for example, was charged with “the dynamite bombing” of a CIA office in Michigan. Keith makes it clear that it would be consistent with the Fourth Amendment for Congress to create different statutory requirements for issuing warrants for surveillance in cases involving domestic security. But Congress has not enacted such rules, and, as a consequence, law enforcement is required to carry out surveillance of criminal activities similar to those in Keith under the requirements of Title III and other parts of ECPA.

This state of affairs remains unaltered by the “lone wolf” amendment to FISA in 2004. That year, Congress amended FISA to include any non-USA person who “engages in international terrorism or activities in preparation therefor” in the definition of “agent of a foreign power.” This revised definition sunsets on December 31, 2009. The change means that the “lone wolf” terrorist need not be tied to a foreign power, but must be a non-USA person engaged in or plotting “international terrorism.” FISA defines “international terrorism” as involving, among other things, activities that “[ō]ccur totally outside the U.S., or transcend national boundaries in terms of the means by which they accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.” 50 U.S.C. §1801(c). As an illustration of the coverage of the “Lone Wolf” amendment, it would not cover Timothy McVeigh, the Oklahoma City bomber.

3. A New Agency for Domestic Intelligence? Francesca Bignami notes that in Europe, one agency is gathered for gathering intelligence on threats abroad posed by foreign governments, and one agency “is charged with gathering intelligence at home, on activities sponsored by foreign powers (counter-intelligence) as well as on home-grown security threats.”16 Both of these agencies are generally overseen not by judiciary, but by legislative and executive branches. Both intelligence agencies generally carry out surveillance under a more permissive set of legal rules than the domestic police. In contrast, in the USA, the FBI is charged with both domestic intelligence investigations and criminal investigations of violations of federal law.

Judge Richard Posner has emerged as the leading critic of the assignment of this

double function to the FBI. The combination of criminal investigation and domestic intelligence at the FBI has not been successful. Posner argues, "If the incompatibility between the law enforcement and intelligence cultures is conceded, then it follows that an agency 100 percent dedicated to domestic intelligence would be likely to do a better job than the FBI, which is at most 20 percent intelligence and thus at least 80 percent criminal investigation and in consequence dominated by the criminal investigations." Posner calls for creation of a "pure" domestic intelligence, one without any law enforcement responsibilities and located outside of the FBI. For Posner, the new U.S. Security Intelligence Surveillance can be modeled on the United Kingdom's MI5 or the Canadian Security Intelligence Service. What should the rules be for such a domestic intelligence agency concerning telecommunications surveillance? Should the FISA rules be applied to it?

C. INTELLIGENCE, TERRORISM, AND NATIONAL SECURITY

1. IS NATIONAL SECURITY DIFFERENT?

p. 302 – Add the following before the paragraph beginning “In 1976 . . .”

Eric Posner and Adrian Vermeule argue that the legislature and judiciary should defer to the executive in times of emergency and that it is justified to curtail civil liberties when national security is threatened:

The essential feature of the emergency is that national security is threatened; because the executive is the only organ of government with the resources, power, and flexibility to respond to threats to national security, it is natural, inevitable, and desirable for power to flow to this branch of government. Congress rationally acquiesces; courts rationally defer . . . . During emergencies, when new threats appear, the balance shifts; government should and will reduce civil liberties in order to enhance security in those domains where the two must be traded off. . . .

In emergencies . . . judges are at sea, even more so than are executive officials. The novelty of the threats and of the necessary responses makes judicial routines and evolved legal rules seem inapposite, even obstructive. There is a premium on the executive’s capacities for swift, vigorous, and secretive action."18

C. INTELLIGENCE, TERRORISM, AND NATIONAL SECURITY

p. 320 – Add the following section after section 5:

6. THE NSA SURVEILLANCE PROGRAM

A front page article in the New York Times in December 2005 first revealed that the NSA was intercepting communications where one party was located outside the U.S. and another party inside the U.S.19 After this story broke, President George W. Bush and

---

Attorney General Alberto Gonzales confirmed, in general terms, this NSA activity. In addition, according to media reports, President Bush signed a secret executive order shortly after the terrorist attack on 9/11. The order authorized NSA access to foreign transit data routed through the U.S. as well as certain foreign-domestic communications. Regarding the foreign-to-foreign communications, exclusively international emails or telephone calls are now sent through telecommunications switches located in the U.S. This routing occurs as a consequence of the growth of fiber optic networks and the digitalization of telecommunications traffic. Today, a telephone call from Dubai to Indonesia may be sent through physical infrastructure located in San Francisco.

President Bush has termed the surveillance of the foreign-domestic communications, the Terrorist Surveillance Program (TSP). Yet, considerable questions exist concerning the precise nature of this program and a host of other secret surveillance programs that may have been in existence at different times. One such secret surveillance program was so controversial that top leadership of the Department of Justice was ready to resign over it in March 2004. At one stage during this period, then White House counsel Alberto Gonzales and White House advisor Andrew Card visited Attorney General Ashcroft, stricken by a medical emergency, in the hospital to attempt to try to have him overrule the Acting Attorney General’s refusal to re-authorize the surveillance program, or some aspect of it. A series of secret negotiations ensued among the White House, Attorney General, and FBI to prevent these resignations and led to changes in the surveillance programs. Notes on these meetings, taken by Director Robert Mueller and released to Congress and the public in heavily-redacted form, has Ashcroft telling Mueller that “he was barred from obtaining the advice he needed on the program by the strict compartmentalization rules” of the White House.

The presidential authorization for the TSP or other surveillance programs has been shared neither with the public nor Congress. The Department of Justice opinions said to declare the activities lawful remain secret. President Bush also has blocked the granting of security clearances to lawyers at the Department of Justice’s Office of Personal Responsibilities (OPR), who were set to investigate the role of DOJ officials in authorizing warrantless NSA surveillance. Attorneys at OPR have never been denied security clearances in the past. Indeed, the Bush administration granted security clearances to “a large team” of prosecutors and FBI agents, in the words of the chief of OPR, to investigate the leaks of information that led to the New York Times disclosure of the program’s existence. During the debate around the Protect America Act of 2007, which amends FISA, the Administration continued to deny Congressional requests for information about the NSA’s warrantless surveillance activities.

There is also the possibility that in one of its US-based programs in the U.S., the NSA is engaged in surveillance of purely domestic communications. In May 2006, USA Today revealed an additional NSA program in which at least one telephone company, AT&T, was providing the NSA with the telephone calling records of tens of millions of Americans. This program is said to involve access to domestic telecommunications

22 Leslie Cauley, NSA Has Massive Database of Americans’ Phone Calls, USA Today, May 11, 2006, at A1. USA Today subsequently admitted that it could not confirm BellSouth and Verizon participation in the NSA program, Frank Ahrens & Howard Kurtz, USA Today Takes Back Some of NSA Phone-Record Report, Wash. Post, July 1, 2006, at A02.
attributes. USA Today reported, “The NSA program reaches into homes and businesses across the nation by amassing information about the calls of ordinary Americans.” Moreover, Seymour Hersh stated that the NSA, subsequent to its program of collecting data about calls, “began to eavesdrop on callers (often using computers to listen for key words) or to investigate them using traditional police methods.”

The information gathered in the NSA programs is then secretly fed back into the established legal system of telecommunications surveillance. According to James Risen, the Bush administration obtains FISA court approval for wiretaps “in part on the basis of information gathered from the earlier warrantless eavesdropping.” Two of his sources estimated that approximately ten to twenty percent of the annual FISA warrants are based on information garnered through the NSA domestic surveillance program. In summary, there may be several programs in which the NSA is engaged in surveillance within the U.S., including some in which data mining is used.

After claiming that its surveillance activity could not be made compatible with FISA, the Bush administration changed course in January 2007 and announced that it had brought at least one of its surveillance programs under the FISC’s supervision. In May 2007, Mitchell McConnell, the Director of National Intelligence, also informed Congress that the Bush Administration would not commit itself to continue seeking FISA warrants.

At some time in Spring 2007, a secret FISC decision denied permission for certain NSA’s surveillance activities. The FISC judgment was said to concern a NSA request for a so-called “basket warrant,” under which warrants are issued not on a case-by-case basis for specific suspects, but more generally for surveillance activity involving multiple targets. One anonymous official was quoted as saying that the FISC ruling concerned cases “where one end is foreign and you don’t know where the other is.”

The Administration leaked information about this ruling, made noises about the threat of imminent terrorist attacks, and pressured Congress, controlled by Democrats with majorities in both houses, to enact the Protect America Act before going on its summer recess in August 2007. This statute is subject to sunset in 120 days, which guarantees a revisiting of its regulations.

In sum, public information is incomplete and Congress itself enacted the Protect America Act without full knowledge of the administration’s warrantless surveillance. Nonetheless, one can identify three new areas of NSA activities. NSA surveillance appears now to be carried on out (1) foreign-to-foreign communications routed through the U.S. (frequently termed “transit data”); (2) foreign-to-domestic communications; and (3) purely domestic communications. This surveillance activity also likely involve some kind of data mining, that is, computer searches through massive amounts of information to identify links between targets and other patterns that merit further scrutiny.

The Protect America Act creates an exception to FISA’s requirements. The

---

23 Seymour M. Hersh, Listening In: Seymour M. Hersh on the N.S.A.’s Domestic Surveillance Program, The New Yorker 24 (November 15, 2006).
24 Risen, State of War, supra, at 52.
exception is found in the statute’s § 105A. This part of the law exempts all communications “directed at” people outside of the U.S. from FISA’s definition of “electronic surveillance.” Once a communications falls within § 105A, the government may carry it out subject to § 105B and its requirements—rather than FISA and its obligation to seek a warrant from the FISC.

As you read the following excerpt from the Protect America Act, think about the extent to which it covers the different government surveillance programs discussed above.

**THE PROTECT AMERICA ACT**
S. 1927, 110th Cong., 1st Sess.

§105A. Nothing in the definition of electronic surveillance under section 101(f) shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States.

§105B(a). Notwithstanding any other law, the Director of National Intelligence and the Attorney General, may for periods of up to one year authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States if the Director of National Intelligence and the Attorney General determine, based on the information provided to them, that—

1. there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the Court pursuant to section 105C of this Act;
2. the acquisition does not constitute electronic surveillance;
3. the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;
4. a significant purpose of the acquisition is to obtain foreign intelligence information; and
5. the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).

This determination shall be in the form of a written certification, under oath, supported as appropriate by affidavit of appropriate officials in the national security field occupying positions appointed by the President … unless immediate action by the Government is required and time does not permit the preparation of a certification. In such a case, the determination of the Director of National Intelligence and the Attorney General shall be reduced to a certification as soon as possible but in no event more than 72 hours after the determination is made.
§ 105C(a). No later than 120 days after the effective date of this Act, the Attorney General shall submit to the Court established under section 103(a), the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance. The procedures submitted pursuant to this section shall be updated and submitted to the Court on an annual basis.

(b) No later than 180 days after the effective date of this Act, the [Foreign Intelligence Surveillance Court] shall assess the Government’s determination under section 105B(a)(1) that those procedures are reasonably designed to ensure that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance. The court’s review shall be limited to whether the Government’s determination is clearly erroneous.

(c) If the court concludes that the determination is not clearly erroneous, it shall enter an order approving the continued use of such procedures. If the court concludes that the determination is clearly erroneous, it shall issue an order directing the Government to submit new procedures within 30 days or cease any acquisitions under section 105B that are implicated by the court’s order.

(d) The Government may appeal any order issued under subsection (c) to [the Foreign Intelligence Surveillance Court of Review]. If such court determines that the order was properly entered, the court shall immediately provide for the record a written statement of each reason for its decision, and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision. Any acquisitions affected by the order issued under subsection (c) of this section may continue during the pendency of any appeal, the period during which a petition for writ of certiorari may be pending, and any review by the Supreme Court of the United States.

§ 4. On a semi-annual basis the Attorney General shall inform the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives, concerning acquisitions under this section during the previous 6-month period. Each report made under this section shall include--

(1) a description of any incidents of non-compliance with a directive issued by the Attorney General and the Director of National Intelligence under section 105B, to include--

(A) incidents of non-compliance by an element of the Intelligence Community with guidelines or procedures established for determining that the acquisition of foreign intelligence authorized by the Attorney General and Director of National Intelligence concerns persons reasonably to be outside the United States; and

(B) incidents of noncompliance by a specified person to whom the Attorney General and Director of National Intelligence issue a directive under this section; and

(2) the number of certifications and directives issued during the reporting period.

NOTES AND QUESTIONS

1. “Directed at.” The Protect America Act carves out an exception from FISA if surveillance is “directed at a person reasonably believed to be located outside of the
United States.” Such telecommunications surveillance can take place without a FISA-warrant issued by the FISC. It can also sweep in communications with a domestic component if the surveillance itself is not “directed at” the person in the U.S., but the person abroad. The critical term, “directed at,” is not defined in the Act, but left to the Attorney General to shape through creation of “reasonable procedures.” Note as well that a link with an agent of a foreign power or terrorist is not needed; rather, “a significant purpose of the acquisition” must merely be “to obtain foreign intelligence information.” § 105B(4).

As an example of a proposed narrower amendment to the FISA, a competing House Bill in 2007 proposed that “a court order is not required for the acquisition of the contents of any communication between persons that are not located within the United States for the purposes of collecting foreign intelligence information, without respect to whether the communication passes through the United States or the surveillance device is located within the United States.” Improving Foreign Intelligence Surveillance to Defend the Nation and the Constitution Act of 2007, H.R. 3356, 1st Sess., 110th Congress. In a similar fashion, Senator Dianne Feinstein proposed a bill in 2006 that exempted only “foreign-foreign communications” from FISA’s warrant requirements. The Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006, S. 3877, stated, “no court order shall be required for the acquisition through electronic surveillance of the contents of any communication between one person who is not located within the United States and another person who is not located within the United States for the purpose of collecting foreign intelligence information even if such information passes through, or the surveillance device is located within the United States.” Id. at § 301.

2. “Information Structure.” In her analysis of FISA, Patricia Bellia argues that this statute has an “information structure.”28 It comes with “institutional mechanisms” that generate information about the government’s use of it. In a similar fashion, the other telecommunication surveillance statutes have different kinds of rules for reporting about their use.

What is the information structure of the Protect America Act? This statute grants great discretion to the Attorney General, who is to inform four congressional committees on a semi-annual basis of “acquisitions” made under the statute, including incidents of non-compliance. In contrast, the House Bill, discussed in the previous Note, provided a robust audit mechanism. The Attorney General was given a role under it to develop guidelines designed that FISA warrants were sought “when the Attorney General seeks to initiate electronic surveillance, or continue electronic surveillance that began under this section, of a United States person.” The Inspector General of the Department of Justice was then to audit compliance with these guidelines every sixty days and report on the results of these audits to Congress.

3. Exclusivity. FISA provides that it is to be the “exclusive means” for carrying out “electronic surveillance” as defined in the statute. 18 U.S.C. 2511(2)(f). It also states that the statutes governing ordinary law-enforcement investigations, such as Title III, are “exclusive” for the surveillance activities that they regulate. A debate has taken place

---

whether President Bush violated FISA’s exclusivity requirements when he authorized the 
NSA’s warrantless surveillance. The most detailed defense of the Administration came 
in a letter to Congress from the DOJ.29 For an analysis that finds that FISA’s exclusivity 
provision prohibits such surveillance, see David S. Kris, Testimony, U.S. Senate 
Committee on the Judiciary, NSA III: Wartime Executive Powers and the FISA Court 
(March 28, 2006).

In one reading of the Protect America Act, it has legislated out of existence the 
“exclusivity” question -- at least for future NSA activity. Recall that warrantless 
surveillance activity that falls under Section 105B is not “electronic surveillance” under 
FISA, which means that FISA’s exclusivity provision do not apply to it. The President 
can therefore argue that he has constitutional authority under Article II to carry out this 
surveillance -- in addition, to any authority that the Protect America Act grants him.

4. Litigation. Several courts have heard challenges to the NSA warrantless 
wiretapping. The Sixth Circuit reversed a district court opinion that barred further use 
operation of TSP. ACLU v. NSA, -- F. 3d – , 2007 WL 1952370 (6th Cir. 2007). The 6th 
Circuit found that plaintiffs lacked standing to bring their claims, and that NSA’s use of 
warrantless wiretaps violated neither FISA nor Title III. In dissent, Judge Ronald Gilman 
found that plaintiffs had standing to challenge the program. Gillman’s dissent also 
argued that TSP violated FISA and Title III.

2006), the court found that plaintiffs had standing. The plaintiffs in that case said that 
they had evidence providing their communications had been intercepted; the court found 
that the “plaintiffs should have an opportunity to establish standing and make a prima 
facie case, even if they must do so in camera.” In contrast, in Tooley v. Bush, 2006 WL 
3783142 (D.D.C. 2006), the court found that the plaintiff did not prove any factual basis 
for his statement that he had been the subject of illegal wiretaps and therefore lacked 
standing.

Plaintiffs have also sued telecommunications providers for their participation in 
the government’s warrantless surveillance activities. In Hepting v. AT&T, 439 F. Supp. 
2d 974, 999-1000 (N.D. Cal. 2006), the district court found plaintiffs’ had standing to sue 
a telecommunications company for providing the NSA with access to their records. The 
9th Circuit has heard an appeal from this judgment. In contrast, the court in Terkel v. 
At&T, 441 F. Supp. 2d 899 (N.D. Ill. 2006), found that the plaintiffs lacked standing 
against AT&T because of their inability to prove that AT&T had disclosed their records 
to the government.

5. The End of FISA? Writing shortly before the enactment of the Protect 
America Act, one scholar proclaimed the demise of FISA due to the NSA’s warrantless 
wiretapping, William Banks argues: “At a minimum, the unraveling of FISA and 
emergence of the TSP call into question the virtual disappearance of effective oversight 
of our national security surveillance. The Congress and federal courts have become 
observers of the system, not even participants, much less overseers.”30 He proposes: “If

29 Letter from William E. Moschella, Asst. Attorney General, to Pat Roberts, Chairman, Select Committee on 
Intelligence, Dec. 22, 2005.
30 William C. Banks, The Death of FISA, 91 Minn. L. Rev. 1209, 1297 (2007).
FISA is to have any meaningful role for the next thirty years, its central terms will have to be restored, one way or another.”

In contrast, John Yoo argues that such surveillance should be permitted where there is a reasonable chance that terrorists will appear, or communicate, even if we do not know their specific identities. Yoo argues that in cases where there is a likelihood, perhaps “a 50 percent chance” that terrorists would use a certain kind of avenue for reaching each other, “[a] FISA-based approach would prevent computers from searching through that channel for keywords or names that might suggest terrorist communications.”

E. GOVERNMENT COMPUTER SEARCHES

p. 325 – Add the following heading before Shared Computers; renumber subsequent sections:

2. SHARED COMPUTERS AND PASSWORD PROTECTION

Begin this section with the brief discussion of Trulock v. Freeh in the casebook on p. 325. Then add:

UNITED STATES v. ANDRUS
483 F.3d 711 (10th Cir. 2007)

[Federal authorities believed that Ray Andrus was downloading child pornography to his home computer. Ray Andrus resided at his parents’ house. Federal officials obtained the consent of Dr. Andrus (Andrus’s father) to search the home. He also consented to their searching any computers in the home. The officials went into Ray Andrus’s bedroom and a forensic expert examined the contents of the computer’s hard drive with forensic software. The software enabled direct access to the computer, bypassing any password protection the user put on it. The officials discovered child pornography on the computer. Later on, the officials learned that Ray Andrus had protected his computer with a password and that his father did not know the password. Is the father’s consent to search the computer valid since he did not know the password?]

MURPHY, J. . . . Subject to limited exceptions, the Fourth Amendment prohibits warrantless searches of an individual’s home or possessions. Voluntary consent to a police search, given by the individual under investigation or by a third party with authority over the subject property, is a well-established exception to the warrant requirement. Valid third party consent can arise either through the third party’s actual authority or the third party’s apparent authority. A third party has actual authority to consent to a search “if that third party has either (1) mutual use of the property by virtue of joint access, or (2) control for most purposes.” Even where actual authority is lacking, however, a third party has apparent authority to consent to a search when an officer

31 John Yoo, War By Other Means: An Insider’s Accounts of the War on Terror 112 (2006).
reasonably, even if erroneously, believes the third party possesses authority to consent. See Georgia v. Randolph, 547 U.S. 103 (2006).

Whether apparent authority exists is an objective, totality-of-the-circumstances inquiry into whether the facts available to the officers at the time they commenced the search would lead a reasonable officer to believe the third party had authority to consent to the search. When the property to be searched is an object or container, the relevant inquiry must address the third party’s relationship to the object. In Randolph, the Court explained, “The constant element in assessing Fourth Amendment reasonableness in consent cases . . . is the great significance given to widely shared social expectations.” For example, the Court said, “[W]hen it comes to searching through bureau drawers, there will be instances in which even a person clearly belonging on the premises as an occupant may lack any perceived authority to consent.”

It may be unreasonable for law enforcement to believe a third party has authority to consent to the search of an object typically associated with a high expectation of privacy, especially when the officers know or should know the owner has indicated the intent to exclude the third party from using or exerting control over the object.

Courts considering the issue have attempted to analogize computers to other items more commonly seen in Fourth Amendment jurisprudence. Individuals’ expectations of privacy in computers have been likened to their expectations of privacy in “a suitcase or briefcase.” Password-protected files have been compared to a “locked footlocker inside the bedroom.” Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir.2001).

Given the pervasiveness of computers in American homes, this court must reach some, at least tentative, conclusion about the category into which personal computers fall. A personal computer is often a repository for private information the computer’s owner does not intend to share with others.

The inquiry into whether the owner of a highly personal object has indicated a subjective expectation of privacy traditionally focuses on whether the subject suitcase, footlocker, or other container is physically locked. Determining whether a computer is “locked,” or whether a reasonable officer should know a computer may be locked, presents a challenge distinct from that associated with other types of closed containers. Unlike footlockers or suitcases, where the presence of a locking device is generally apparent by looking at the item, a “lock” on the data within a computer is not apparent from a visual inspection of the outside of the computer, especially when the computer is in the “off” position prior to the search. Data on an entire computer may be protected by a password, with the password functioning as a lock, or there may be multiple users of a computer, each of whom has an individual and personalized password-protected “user profile.”

Courts addressing the issue of third party consent in the context of computers, therefore, have examined officers’ knowledge about password protection as an indication of whether a computer is “locked” in the way a footlocker would be. For example, in Trulock, the Fourth Circuit held a live-in girlfriend lacked actual authority to consent to a search of her boyfriend’s computer files where the girlfriend told police she and her boyfriend shared the household computer but had separate password-protected files that were inaccessible to the other. The court in that case explained, “Although Conrad had authority to consent to a general search of the computer, her authority did not extend to Trulock’s password-protected files.”
In addition to password protection, courts also consider the location of the computer within the house and other indicia of household members’ access to the computer in assessing third party authority. Third party apparent authority to consent to a search has generally been upheld when the computer is located in a common area of the home that is accessible to other family members under circumstances indicating the other family members were not excluded from using the computer. In contrast, where the third party has affirmatively disclaimed access to or control over the computer or a portion of the computer’s files, even when the computer is located in a common area of the house, courts have been unwilling to find third party authority.

Andrus’ case presents facts that differ somewhat from those in other cases. Andrus’ computer was located in a bedroom occupied by the homeowner’s fifty-one year old son rather than in a true common area. Dr. Andrus, however, had unlimited access to the room. Law enforcement officers did not ask specific questions about Dr. Andrus’ use of the computer, but Dr. Andrus said nothing indicating the need for such questions. Cf. Trulock, 275 F.3d at 398 (when law enforcement questioned third party girlfriend about computer, she indicated she and boyfriend had separate password-protected files).

The resolution of this appeal turns on whether the officers’ belief in Dr. Andrus’ authority was reasonable, despite the lack of any affirmative assertion by Dr. Andrus that he used the computer and despite the existence of a user profile indicating Ray Andrus’ intent to exclude other household members from using the computer. For the reasons articulated below, this court concludes the officers’ belief in Dr. Andrus’ authority was reasonable.

First, the officers knew Dr. Andrus owned the house and lived there with family members. Second, the officers knew Dr. Andrus’ house had internet access and that Dr. Andrus paid the Time Warner internet and cable bill. Third, the officers knew the email address bandrus@kc.rr.com had been activated and used to register on a website that provided access to child pornography. Fourth, although the officers knew Ray Andrus lived in the center bedroom, they also knew that Dr. Andrus had access to the room at will. Fifth, the officers saw the computer in plain view on the desk in Andrus’ room and it appeared available for use by other household members. Furthermore, the record indicates Dr. Andrus did not say or do anything to indicate his lack of ownership or control over the computer when Cheatham asked for his consent to conduct a computer search. It is uncontested that Dr. Andrus led the officers to the bedroom in which the computer was located, and, even after he saw Kanatzar begin to work on the computer, Dr. Andrus remained silent about any lack of authority he had over the computer. Even if Ray Andrus’ computer was protected with a user name and password, there is no indication in the record that the officers knew or had reason to believe such protections were in place.

Andrus argues his computer’s password protection indicated his computer was “locked” to third parties, a fact the officers would have known had they asked questions of Dr. Andrus prior to searching the computer. Under our case law, however, officers are not obligated to ask questions unless the circumstances are ambiguous. In essence, by suggesting the onus was on the officers to ask about password protection prior to searching the computer, despite the absence of any indication that Dr. Andrus’ access to the computer was limited by a password, Andrus necessarily submits there is inherent ambiguity whenever police want to search a household computer and a third party has not
affirmatively provided information about his own use of the computer or about password protection. Andrus’ argument presupposes, however, that password protection of home computers is so common that a reasonable officer ought to know password protection is likely. Andrus has neither made this argument directly nor proffered any evidence to demonstrate a high incidence of password protection among home computer users.

Viewed under the requisite totality-of-the-circumstances analysis, the facts known to the officers at the time the computer search commenced created an objectively reasonable perception that Dr. Andrus was, at least, one user of the computer. That objectively reasonable belief would have been enough to give Dr. Andrus apparent authority to consent to a search. Even if Dr. Andrus had no actual ability to use the computer and the computer was password protected, these mistakes of fact do not negate a determination of Dr. Andrus’ apparent authority. In this case, the district court found Agent Cheatham properly halted the search when further conversation with Dr. Andrus revealed he did not use the computer and that Andrus’ computer was the only computer in the house. These later revelations, however, have no bearing on the reasonableness of the officers’ belief in Dr. Andrus’ authority at the outset of the computer search.

MCKAY, J. DISSENTING. This case concerns the reasonable expectation of privacy associated with password-protected computers. In examining the contours of a third party’s apparent authority to consent to the search of a home computer, the majority correctly indicates that the extent to which law enforcement knows or should reasonably suspect that password protection is enabled is critical. I take issue with the majority’s implicit holding that law enforcement may use software deliberately designed to automatically bypass computer password protection based on third-party consent without the need to make a reasonable inquiry regarding the presence of password protection and the third party’s access to that password.

The presence of security on Defendant’s computer is undisputed. Yet, the majority curiously argues that Defendant’s use of password protection is inconsequential because Defendant failed to argue that computer password protection is “commonplace.” Of course, the decision provides no guidance on what would constitute sufficient proof of the prevalence of password protection, nor does it explain why the court could not take judicial notice that password protection is a standard feature of operating systems. Despite recognizing the “pervasiveness of computers in American homes,” and the fact that the “personal computer is often a repository for private information the computer’s owner does not intend to share with others,” the majority requires the invocation of magical language in order to give effect to Defendant’s subjective intent to exclude others from accessing the computer.

The unconstrained ability of law enforcement to use forensic software such as the EnCase program to bypass password protection without first determining whether such passwords have been enabled does not “exacerbate[ ]” this difficulty; rather, it avoids it altogether, simultaneously and dangerously sidestepping the Fourth Amendment in the process. Indeed, the majority concedes that if such protection were “shown to be commonplace, law enforcement’s use of forensic software like EnCase . . . may well be subject to question.” But the fact that a computer password “lock” may not be immediately visible does not render it unlocked. I appreciate that unlike the locked file cabinet, computers have no handle to pull. But, like the padlocked footlocker, computers
do exhibit outward signs of password protection: they display boot password screens, username/password log-in screens, and/or screen-saver reactivation passwords.

The fact remains that EnCase’s ability to bypass security measures is well known to law enforcement. Here, ICE’s forensic computer specialist found Defendant’s computer turned off. Without turning it on, he hooked his laptop directly to the hard drive of Defendant’s computer and ran the EnCase program. The agents made no effort to ascertain whether such security was enabled prior to initiating the search. . . .

The majority points out that law enforcement “did not ask specific questions” about Dr. Andrus’ use of the computer or knowledge of Ray Andrus’ use of password protection, but twice criticizes Dr. Andrus’ failure to affirmatively disclaim ownership of, control over, or knowledge regarding the computer. Of course, the computer was located in Ray Andrus’ very tiny bedroom, but the majority makes no effort to explain how this does not create an ambiguous situation as to ownership.

The burden on law enforcement to identify ownership of the computer was minimal. A simple question or two would have sufficed. Prior to the computer search, the agents questioned Dr. Andrus about Ray Andrus’ status as a renter and Dr. Andrus’ ability to enter his 51-year-old son’s bedroom in order to determine Dr. Andrus’ ability to consent to a search of the room, but the agents did not inquire whether Dr. Andrus used the computer, and if so, whether he had access to his son’s password. At the suppression hearing, the agents testified that they were not immediately aware that Defendant’s computer was the only one in the house, and they began to doubt Dr. Andrus’ authority to consent when they learned this fact. The record reveals that, upon questioning, Dr. Andrus indicated that there was a computer in the house and led the agents to Defendant’s room. The forensic specialist was then summoned. It took him approximately fifteen to twenty minutes to set up his equipment, yet, bizarrely, at no point during this period did the agents inquire about the presence of any other computers. . . .

Accordingly, in my view, given the case law indicating the importance of computer password protection, the common knowledge about the prevalence of password usage, and the design of EnCase or similar password bypass mechanisms, the Fourth Amendment and the reasonable inquiry rule, mandate that in consent-based, warrantless computer searches, law enforcement personnel inquire or otherwise check for the presence of password protection and, if a password is present, inquire about the consenter’s knowledge of that password and joint access to the computer. . . .
NOTES & QUESTIONS

1. *A Question of Perspective?* Orin Kerr contends:

   From a virtual user’s perspective, the child pornography was hidden to the father; it was behind a password-protected gate. Under these facts, the father couldn’t consent to a search because he would lack common authority over it. From a physical perspective, however, the file was present on the hard drive just like all the other information. Under these facts, the father could consent to the search because he had access rights to the machine generally. . . .

   Viewed from the physical perspective, the investigators reasonably did not know about the user profile and reasonably believed that the father had rights to consent to that part of the hard drive.  

2. *Checking for Password Protection.* Was the investigators’ belief about the father’s authority over the computer reasonable? Should the investigators have asked the father more questions about his use of the computer first? Should they have turned on the machine to see if it was password-protected before hooking up the forensic software? What kinds of incentives does this decision engender for officers doing an investigation?

p. 338 – Add new Section 3: Email; renumber other sections; insert text below:

3. EMAIL

   **WARSHAK v. UNITED STATES**
   -- F.3d --, 2007 WL 1730094 (6th Cir. 2007)

   Martin, J. . . . The government appeals the district court’s entry of a preliminary injunction, prohibiting it from seizing “the contents of any personal e-mail account maintained by an Internet Service Provider in the name of any resident of the Southern District of Ohio without providing the relevant account holder or subscriber prior notice and an opportunity to be heard on any complaint, motion, or other pleading seeking issuance of such an order.” For the reasons discussed below, we largely affirm the district court’s decision, requiring only that the preliminary injunction be slightly modified on remand.

   In March 2005, the United States was engaged in a criminal investigation of Plaintiff Steven Warshak and the company he owned, Berkeley Premium Nutraceuticals, Inc. The investigation pertained to allegations of mail and wire fraud, money laundering, and related federal offenses. On May 6, 2005, the government obtained an order from a United States Magistrate Judge in the Southern District of Ohio directing internet service provider (“ISP”) NuVox Communications to turn over to government agents information pertaining to Warshak’s e-mail account with NuVox. The information to be disclosed included (1) customer account information, such as application information, “account identifiers,” “[b]illing information to include bank account numbers,” contact information, and “[a]ny other information pertaining to the customer, including set up, synchronization, etc.”; (2) “[t]he contents of wire or electronic communications (not in electronic storage unless greater than 181 days old) that were placed or stored in

---

directories or files owned or controlled” by Warshak; and (3) “[a]ll Log files and backup tapes.”

The order stated that it was issued under 18 U.S.C. § 2703, part of the Stored Communications Act (“SCA”), and that it was based on “specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.” The order was issued under seal, and prohibited NuVox from “disclos[ing] the existence of the Application or this Order of the Court, or the existence of this investigation, to the listed customer or to any person unless and until authorized to do so by the Court.” The magistrate further ordered that “the notification by the government otherwise required under 18 U.S.C. § 2703(b)(1)(B) be delayed for ninety days.” On September 12, 2005, the government obtained a nearly identical order pertaining to Yahoo, another ISP, that sought the same types of information from Warshak’s Yahoo e-mail account and a Yahoo account identified with another individual named Ron Fricke.

On May 31, 2006, over a year after obtaining the NuVox order, the United States wrote to Warshak to notify him of both orders and their requirements. The magistrate had unsealed both orders the previous day. Based on this disclosure, Warshak filed suit on June 12, 2006, seeking declaratory and injunctive relief, and alleging that the compelled disclosure of his e-mails without a warrant violated the Fourth Amendment and the SCA. After filing the complaint, Warshak’s counsel sought the government’s assurance that it would not seek additional orders under section 2703(d) directed at his e-mails, at least for some discrete period of time during the pendency of his civil suit. The government declined to provide any such assurance. In response, Warshak moved for a temporary restraining order and/or a preliminary injunction prohibiting such future searches. The district court held a telephonic hearing on the motions, and eventually granted part of the equitable relief sought by Warshak.

The government appeals from the district court’s ruling.

The SCA, passed by Congress in 1986, is codified at 18 U.S.C. §§ 2701 to 2712, and contains a number of provisions pertaining to the accessibility of “stored wire and electronic communications and transactional records.” At issue in this case is § 2703, which provides procedures through which a governmental entity can access both user records and other subscriber information, and the content of electronic messages.

With respect to the merits of the preliminary injunction, the government argues that court orders issued under section 2703 are not searches but rather compelled disclosures, akin to subpoenas. As a result, according to the government, the more stringent showing of probable cause, a prerequisite to the issuance of a warrant under the Fourth Amendment, is inapplicable, and an order under section 2703 need only be supported by a showing of “reasonable relevance.”

Where the party challenging the disclosure has voluntarily disclosed his records to a third party, he maintains no expectation of privacy in the disclosure vis-a-vis that individual, and assumes the risk of that person disclosing (or being compelled to disclose) the shared information to the authorities. See, e.g., United States v. Jacobsen, 466 U.S. 109, 117 (1984) (“[W]hen an individual reveals private information to another, he

33 The government has conceded that it violated the statute by waiting for over a year without providing notice of the e-mail seizures to Warshak or seeking extensions of the delayed notification period, and it appears to have violated the magistrate’s decision for the same reason.
assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information.").

Combining this disclosure to a third party with the government’s ability to subpoena the third party alleviates any need for the third-party subpoena to meet the probable cause requirement, if the challenger has not maintained an expectation of privacy with respect to the individual being compelled to make the disclosure. … The government’s compelled disclosure argument, while relevant, therefore begs the critical question of whether an e-mail user maintains a reasonable expectation of privacy in his e-mails vis-a-vis the party who is subject to compelled disclosure—in this instance, the ISPs. If he does not, …then the government must meet only the reasonableness standard applicable to compelled disclosures to obtain the material. If, on the other hand, the e-mail user does maintain a reasonable expectation of privacy in the content of the e-mails with respect to the ISP, then the Fourth Amendment’s probable cause standard controls the e-mail seizure.

Two amici curiae convincingly analogize the privacy interest that e-mail users hold in the content of their e-mails to the privacy interest in the content of telephone calls, recognized by the Supreme Court in its line of cases involving government eavesdropping on telephone conversations. See Smith v. Maryland, 442 U.S. 735 (1979); Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967). In Berger and Katz, telephone surveillance that intercepted the content of a conversation was held to constitute a search, because the caller “is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,” and therefore cannot be said to have forfeited his privacy right in the conversation. Katz, 389 U.S. at 352. This is so even though “[t]he telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment.” Smith, 442 U.S. at 746 (Stewart, J., dissenting). On the other hand, in Smith, the Court ruled that the use of pen register, installed at the phone company’s facility to record the numbers dialed by the telephone user, did not amount to a search. This distinction was due to the fact that “a pen register differs significantly from the listening device employed in Katz, for pen registers do not acquire the contents of communications.” 442 U.S. at 741 (emphasis in original).

The distinction between Katz and Miller makes clear that the reasonable expectation of privacy inquiry in the context of shared communications must necessarily focus on two narrower questions than the general fact that the communication was shared with another. First, we must specifically identify the party with whom the communication is shared, as well as the parties from whom disclosure is shielded. Clearly, under Katz, the mere fact that a communication is shared with another person does not entirely erode all expectations of privacy, because otherwise eavesdropping would never amount to a search. It is true, however, that by sharing communications with someone else, the speaker or writer assumes the risk that it could be revealed to the government by that person, or obtained through a subpoena directed to that person. See Miller, 425 U.S. at 443 (“[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.”). The same does not

34 Editor’s Note: The 6th Circuit here refers to a brief by amici curiae Professors Patricia Bellia, Notre Dame Law School, and Susan Freiwald, University of San Francisco School of Law.
necessarily apply, however, to an intermediary that merely has the ability to access the information sought by the government. Otherwise phone conversations would never be protected, merely because the telephone company can access them; letters would never be protected, by virtue of the Postal Service’s ability to access them; the contents of shared safe deposit boxes or storage lockers would never be protected, by virtue of the bank or storage company’s ability to access them.

The second necessary inquiry pertains to the precise information actually conveyed to the party through whom disclosure is sought or obtained. This distinction provides the obvious crux for the different results in *Katz* and *Smith*, because although the conduct of the telephone user in *Smith* “may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.” 442 U.S. at 743. Like the depositor in *Miller*, the caller in *Smith* “assumed the risk” of the phone company disclosing the records that he conveyed to it. Yet this assumption of the risk is limited to the specific information conveyed to the service provider, which in the telephone context excludes the content of the conversation. It is apparent, therefore, that although the government can compel disclosure of a shared communication from the party with whom it was shared, it can only compel disclosure of the specific information to which the subject of its compulsion has been granted access. It cannot, on the other hand, bootstrap an intermediary’s limited access to one part of the communication (e.g. the phone number) to allow it access to another part (the content of the conversation).

This focus on the specific information shared with the subject of compelled disclosure applies with equal force in the e-mail context. Compelled disclosure of subscriber information and related records through the ISP might not undermine the e-mail subscriber’s Fourth Amendment interest under *Smith*, because like the information obtained through the pen register in *Smith* and like the bank records in *Miller*, subscriber information and related records are records of the service provider as well, and may likely be accessed by ISP employees in the normal course of their employment. Consequently, the user does not maintain the same expectation of privacy in them vis-a-vis the service provider, and a third party subpoena to the service provider to access information that is shared with it likely creates no Fourth Amendment problems. FN3 The combined precedents of *Katz* and *Smith*, however, recognize a heightened protection for the content of the communications. Like telephone conversations, simply because the phone company or the ISP could access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course.

Similarly, under both *Miller* and *Katz*, if the government in this case had received the content of Warshak’s e-mails by subpoenaing the person with whom Warshak was e-mailing, a Fourth Amendment challenge brought by Warshak would fail, because he would not have maintained a reasonable expectation of privacy vis-a-vis his e-mailing partners. But this rationale is inapplicable where the party subpoenaed is not expected to access the content of the documents, much like the phone company in *Katz*. Thus, as Warshak argues, the government could not get around the privacy interest attached to a private letter by simply subpoenaing the postal service with no showing of probable cause, because unlike in *Phibbs*, postal workers would not be expected to read the letter in the normal course of business. ... Similarly, a bank customer maintains an expectation
of privacy in a safe deposit box to which the bank lacks access (as opposed to bank records, like checks or account statements) and the government could not compel disclosure of the contents of the safe deposit box only by subpoenaing the bank. …

Turning to the instant case, we have little difficulty agreeing with the district court that individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP. The content of e-mail is something that the user “seeks to preserve as private,” and therefore “may be constitutionally protected.” [Katz], 389 U.S. at 351. It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past. …

The government asserts that ISPs have the contractual right to access users’ e-mails. The district court’s ruling was based on its willingness to credit Warshak’s contrary factual argument that “employees of commercial ISPs [do not] open and read-[nor do] their subscribers reasonably expect them to open and read-individual subscriber e-mails as a matter of course.” … [T]he terms of service in question here, which the government has cited to in both the district court and this Court, clearly provide for access only in limited circumstances, rather than wholesale inspection, auditing, or monitoring of e-mails. Because the ISPs right to access e-mails under these user agreements is reserved for extraordinary circumstances, … it is similarly insufficient to undermine a user’s expectation of privacy. For now, the government has made no showing that e-mail content is regularly accessed by ISPs, or that users are aware of such access of content.

The government also insists that ISPs regularly screen users’ e-mails for viruses, spam, and child pornography. Even assuming that this is true, however, such a process does not waive an expectation of privacy in the content of e-mails sent through the ISP, for the same reasons that the terms of service are insufficient to waive privacy expectations. … The fact that a computer scans millions of e-mails for signs of pornography or a virus does not invade an individual’s content-based privacy interest in the e-mails and has little bearing on his expectation of privacy in the content. In fact, these screening processes are analogous to the post office screening packages for evidence of drugs or explosives, which does not expose the content of written documents enclosed in the packages. The fact that such screening occurs as a general matter does not diminish the well-established reasonable expectation of privacy that users of the mail maintain in the packages they send. …

The government’s compelled disclosure argument is initially on point, but fails to address adequately the caveat relating to a party’s maintenance of a reasonable expectation of privacy in documents in the custody of a third party. A warrant based on probable cause would not have been necessary had the government subpoenaed Warshak or given him prior notice of its intent to seek an SCA order, because the need for this higher showing would be offset by his ability to obtain judicial review before producing any e-mails. …The same rationale would apply if the government subpoenaed a third party that had access to the content of the e-mails, and against whom Warshak had no claim of privacy, such as the recipient of one of his e-mails. By the same token, an SCA order that provided notice to the ISP alone, and not to the user, would be appropriate in the limited instances where the user had waived his expectation of privacy with respect to
the ISP, such as where the government can show that auditing, monitoring, or inspection are expressly provided for in the terms of service, or where the user has e-mailed content directly to the ISP. Where the third party is not expected to access the e-mails in the normal course of business, however, the party maintains a reasonable expectation of privacy, and subpoenaing the entity with mere custody over the documents is insufficient to trump the Fourth Amendment warrant requirement.

The district court enjoined the United States “from seizing, pursuant to court order under 18 U.S.C. § 2703(d), the contents of any personal e-mail account maintained by an Internet Service Provider in the name of any resident of the Southern District of Ohio without providing the relevant account holder or subscriber prior notice and an opportunity to be heard. . . . “ Our discussion above necessitates one modification to this injunction, which counsel for Warshak agreed at oral argument would be appropriate. If the government can show, based on specific facts, that an e-mail account holder has waived his expectation of privacy vis-a-vis the ISP, compelled disclosure of e-mails through notice to the ISP alone would be appropriate. This is a narrow modification, however, as a right to access e-mails in an account only in certain limited circumstances would not be sufficient. Rather, the government must show that the ISP or other intermediary clearly established and utilized the right to inspect, monitor, or audit the content of e-mails, or otherwise had content revealed to it. In such cases the SCA order will operate as the functional equivalent of a third party subpoena, allowing disclosure through a party that has total access to the documents in question. On remand, therefore, the preliminary injunction shall allow seizures of e-mail in three situations: (1) if the government obtains a search warrant under the Fourth Amendment, based on probable cause and in compliance with the particularity requirement; (2) if the government provides notice to the account holder in seeking an SCA order, according him the same judicial review he would be allowed were he to be subpoenaed; or (3) if the government can show specific, articulable facts, demonstrating that an ISP or other entity has complete access to the e-mails in question and that it actually relies on and utilizes this access in the normal course of business, sufficient to establish that the user has waived his expectation of privacy with respect to that entity, in which case compelled disclosure may occur if that entity is afforded notice and an opportunity to be heard.

The district court correctly determined that e-mail users maintain a reasonable expectation of privacy in the content of their e-mails, and we agree that the injunctive relief it crafted was largely appropriate, although we find necessary one modification. On remand, the preliminary injunction should be modified to prohibit the United States from seizing the contents of a personal e-mail account maintained by an ISP in the name of any resident of the Southern District of Ohio, pursuant to a court order issued under 18 U.S.C. § 2703(d), without either (1) providing the relevant account holder or subscriber prior notice and an opportunity to be heard, or (2) making a fact-specific showing that the account holder maintained no expectation of privacy with respect to the ISP, in which case only the ISP need be provided prior notice and an opportunity to be heard.
CHAPTER 4: HEALTH AND GENETIC PRIVACY

SUMMARY OF ADDITIONS TO CHAPTER

• In B.6 (HIPAA), we added a note about State ex. Rel Cincinnati Enquirer v. Daniels, a case involving whether HIPAA barred the public disclosure of certain health information.

B. CONFIDENTIALITY OF MEDICAL INFORMATION
6. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

p. 394 – Add the following note after note 2:

3. HIPAA vs. Public Access to Government Information. In State ex. rel Cincinnati Enquirer v. Daniels, 844 N.E.2d 1181 (Ohio 2006), a newspaper sought to obtain copies of lead citation notices “issued to property owners of units reported to be the residences of children whose blood tests indicated elevated lead levels.” The Cincinnati Health Department denied the newspaper’s request, claiming that it was barred from disclosing the data because it was “protected health information” under HIPAA. The Ohio Supreme Court concluded:

For the first time, we address the conflict-of-laws poser where a state public-records law, here R.C. 149.43, requires disclosure of a public record, while federal law, HIPAA and its privacy rule, specifically prohibits disclosure of protected health information. . . .

Section 160.103, Title 45, C.F.R. defines “health information” to include information created by a public health authority that relates to the past, present, or future physical condition of an individual.

. . . [T]he lead-citation notices issued by the health department reveal that they are intended to advise the owners of real estate about results of department investigations and to apprise them of violations relating to lead hazards; the report identifies existing and potential lead hazards on the exterior and interior of the property, details the tests performed on the property and the results of those tests, explains the abatement measures required, provides advice about options to correct the problem, and mandates reporting of abatement measures, including the name of the abatement contractor, the abatement method, and the date of expected abatement completion. Nothing contained in these reports identifies by name, age, birth date, social security number, telephone number, family information, photograph, or other identifier any specific individual or details any specific medical examination, assessment, diagnosis, or treatment of any medical condition. There is a mere nondescript reference to “a” child with “an” elevated lead level. . . .

The prohibition against disclosure contained in the HIPAA privacy rule refers to the release of otherwise protected health information. It provides: “A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.” Section 164.502(a), Title 45, C.F.R. After careful review of the
record, we have concluded that the lead-risk-assessment reports and the lead citations do not contain protected health information and therefore are subject to release, as they are not protected by the HIPAA privacy rule.

However, even if the records did contain protected health information, they would still be subject to release in accordance with the “required by law” exception to HIPAA.

HIPAA contains definitions with respect to classification of entities as either performing operations that are covered by its provisions or performing hybrid operations, some of which may not be covered by its provisions.

The Cincinnati Health Department urges in this regard that pursuant to Section 160.103, Title 45, C.F.R., it is a covered entity as defined by HIPAA and as such may not use or disclose protected health information except as provided for in HIPAA. The Enquirer claims, on the other hand, that the Cincinnati Health Department is a “hybrid entity” as that term is defined in Section 164.103, Title 45, C.F.R., i.e., an entity whose business actions include both covered and noncovered functions as defined by HIPAA. Section 164.502(a) refers to a “covered entity” and provides that it “may not use or disclose protected health information,” except as permitted or required by law.

This analysis, however, becomes relevant only if we conclude that the health department is a hybrid entity performing a noncovered action. Assuming for the sake of argument that the health department is a covered entity as it claims, the next part of our analysis requires us to review the claim of the director of health that the information contained in the lead-citation notices constitutes “protected health information.”

Specifically, Section 164.514(a), Title 45, C.F.R. provides: “Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.”

The department contends that the single sentence contained in its notice of citation regarding the residence of a child with an elevated blood lead level constitutes a “reasonable basis to believe that the information can be used to identify an individual” and therefore that the citations are not subject to disclosure. We disagree.

A review of HIPAA reveals a “required by law” exception to the prohibition against disclosure of protected health information. With respect to this position, Section 164.512(a)(1), Title 45, C.F.R. provides, “A covered entity may . . . . disclose protected health information to the extent that such . . . disclosure is required by law.” (Emphasis added.) And the Ohio Public Records Act requires disclosure of records unless the disclosure or release is prohibited by federal law. R.C. 149.43(a)(1)(v).

Hence, we are confronted here with a problem of circular reference because the Ohio Public Records Act requires disclosure of information unless prohibited by federal law, while federal law allows disclosure of protected health information if required by state law. FN1

Our research reveals that at the time of implementing these regulations, the Department of Health and Human Services, Office of the Secretary, promulgated Standards for Privacy of Individually Identifiable Health Information (2000), 65 F.R. 82462, 82667-82668, stating, “[W]e intend [160.512(a) ] to preserve access to information considered important enough by state or federal authorities to require its disclosure by law”; “we do not believe that Congress intended to preempt each such law”; and “[t]he rule’s approach is simply intended to avoid any obstruction to the health plan or covered health care provider’s ability to comply with its existing legal obligations.”

Similarly, in reviewing federal Freedom of Information Act (“FOIA”) requests, the secretary explains that federal FOIA requests “come within § 164.512(a) of the privacy regulation that permits uses or disclosures required by law if the uses or disclosures meet the relevant requirements of the law.” (Emphasis added.) 65 F.R. 82462, 82482. By analogy, an entity like the Cincinnati Health Department, faced with an Ohio Public Records Act request, need determine only whether the requested disclosure is required by Ohio law to avoid violating HIPAA’s privacy rule. See, also, Tex.Atty.Gen.Op. 681 (2004) 7, which reached the same conclusion under Texas law; cf. Ohio Legal Rights Serv. v. Buckeye Ranch, Inc. (S.D.Ohio 2005), 365 F.Supp.2d 877, where the court concluded that HIPAA’s “required by law” exception allowed the Ohio Legal Rights Service to access documents relating to the treatment of a mentally ill child pursuant to
Ohio law (R.C. 5123.60) giving the Service “ready access” to those documents.

D. GENETIC INFORMATION

p. 450– Add new notes after note 4:

6. The New Forensics. Erin Murphy proposes that a group of modern forensic sciences, which she terms “second generation sciences,” offers both a new degree of certainty as well as a new potential for misuse:

[E]ven within the short lifetime of the most advanced second-generation science, DNA typing, examples of both questionable methodological assertions and erroneous technical application abound. . . . Both Virginia and Texas wrongly jailed individuals for years on the basis of falsely inculpating DNA evidence. For nearly every laboratory mistake or malfeasant act, there were lawyers and judges who failed to catch it. . . .

As is already apparent from the short history of DNA typing, many of the characteristics that make second-generation sciences so appealing in fact places them at equal, if not greater, risk for error in the current regime.

First, with regard to admissibility determinations, the technical complexity of second-generation techniques make close and continuous judicial scrutiny of their methodological soundness less likely. . . . Even well-meaning judges may struggle to comprehend complicated scientific or mathematical principles, and the heightened likelihood of error may discourage a court from delving too deeply into such complicated scientific knowledge. . . .

Given the rigor of second-generation techniques, defense attorneys, like judges, may find themselves susceptible to the temptation simply to trust the integrity of the evidence, thus making the case seem insurmountable or “open-and-shut.” Many lawyers will reasonably conclude that it requires too great an effort, and reaps too little a reward, to study such evidence in the hopes of uncovering a flawed methodological approach. . . .

[T]he database-dependency of second-generation sciences, and the privacy and proprietary secrets concerns they raise, effectively prohibit access to the material necessary for independent research. Manufacturers of DNA typing kits, cell phone or search engine technologies, or biometric scanning software may bristle at disclosing broadly the technology underlying their particular techniques, even under a court “gag” order. Similarly, the relinquishment of data stored indiscriminately in databanks for exploratory purposes—whether iris patterns, DNA profiles, or cell records—understandably raises legitimate concerns about personal privacy.35

Murphy proposes to loosen “the government’s grip” on the technology. Independent forensic laboratories should be created. Moreover, a centralized oversight group should carry out research and audit functions—and encourage others to pursue these activities as well. Murphy also contends that “the courtroom’s grip on the law” should be loosened. Murphy proposes greater centralization of the defense function to allow pooling of resources. She also advocates defense entitlements to DNA evidence and greater governmental duties, including the burden to place before a trial court continued evidence of a technique’s legitimacy. Do you think these remedies will cure the ills that Murphy has diagnosed in her article?

7. “Abandoned” DNA? Frequently, the law views the police’s collection of discarded DNA as similar to its examination of trash. Recall from Chapter 3.A the case

of *California v. Greenwood*, 486 U.S. 35 (1988), where the Supreme Court held that there was no reasonable expectation of privacy in trash set out at the curb for collection. Law enforcement officials have collected discarded DNA from a smoked cigarette, a recently-used coffee cup, and a licked envelope sent through the mail. Does *Greenwood* foreclose finding a reasonable expectation of a privacy in DNA from discarded items? Should DNA in discarded items be treated similarly to regular trash?

For Elizabeth Joh, however, instead of thinking of the collection and analysis of such samples as involving “abandoned” DNA, we should view it as “covert involuntary DNA sampling.” 36 Joh argues that the law should end its grant of virtually limitless discretion to the police in collecting such DNA. More limits on police procedures are needed in this context because of the vast potential uses of this information, and the rapidity of scientific research in genetics, which makes it difficult to predict the amount of information about an individual that a single genetic sample might reveal. In Joh’s view, the police should be required to obtain a warrant whenever they seek covert involuntary DNA from a target. She also calls for the more modest step of having legislatures clarify “the applicability of DNA database laws, both federal and state, to the collection of abandoned DNA.” 37

---

37 Id. at 881.
CHAPTER 5:
PRIVACY OF ASSOCIATIONS, ANONYMITY,
AND IDENTIFICATION

SUMMARY OF ADDITIONS TO CHAPTER

- In B.2 (anonymity in cyberspace), we include an excerpt of Doe v. Cahill to substitute for Columbia Insurance Co. v. Seescandy.com and Doe v. 2TheMart.com. Doe v. Cahill has more interesting facts and provides a clearly-articulated discussion of the issue of anonymity online. Doe v. 2TheMart.com is preserved but shortened in a footnote after Doe v. Cahill.

B. ANONYMITY
2. ANONYMITY IN CYBERSPACE

pp. 485-489 – Cut Columbia Insurance Co. v. Seescandy.com and Doe v. 2TheMart.com, Inc. and replace with the case below:

DOE V. CAHILL
884 A.2d 451 (Del. 2005)

STEELE, C.J. . . . On November 2, 2004, the plaintiffs below, Patrick and Julia Cahill, both residents of Smyrna, Delaware, filed suit against four John Doe defendants asserting defamation and invasion of privacy claims. This appeal involves only one of the John Doe defendants, John Doe No. 1 below and “Doe” in this opinion. Using the alias “Proud Citizen,” Doe posted two statements on an internet website sponsored by the Delaware State News called the “Smyrna/Clayton Issues Blog” concerning Cahill’s performance as a City Councilman of Smyrna. The “Guidelines” at the top of the blog stated “[t]his is your hometown forum for opinions about public issues.” The first of Doe’s statements, posted on September 18, 2004, said:

If only Councilman Cahill was able to display the same leadership skills, energy and enthusiasm toward the revitalization and growth of the fine town of Smyrna as Mayor Schaeffer has demonstrated! While Mayor Schaeffer has made great strides toward improving the livelihood of Smyrna’s citizens, Cahill has devoted all of his energy to being a divisive impediment to any kind of cooperative movement. Anyone who has spent any amount of time with Cahill would be keenly aware of such character flaws, not to mention an obvious mental deterioration. Cahill is a prime example of failed leadership--his eventual ousting is exactly what Smyrna needs in order to move forward and establish a community that is able to thrive on its own economic stability and common pride in its town.

The next day, Doe posted another statement:
Gahill [sic] is as paranoid as everyone in the town thinks he is. The mayor needs support from his citizens and protections from unfounded attacks.

Pursuant to Superior Court Rule 30, the Cahills sought and obtained leave of the Superior Court to conduct a pre-service deposition of the owner of the internet blog, Independent Newspapers. After obtaining the IP addresses associated with the blog postings from the blog’s owner, the Cahills learned that Comcast Corporation owned Doe’s IP address. An IP address is an electronic number that specifically identifies a particular computer using the internet. IP addresses are often owned by internet service providers who then assign them to subscribers when they use the internet. These addresses are unique and assigned to only one ISP subscriber at a time. Thus, if the ISP knows the time and the date that postings were made from a specific IP address, it can determine the identity of its subscriber.

Armed with Doe’s IP address, the Cahills obtained a court order requiring Comcast to disclose Doe’s identity. As required by Federal Statute, when Comcast received the discovery request, it notified Doe. On January 4, 2005, Doe filed an “Emergency Motion for a Protective Order” seeking to prevent the Cahills from obtaining his identity from Comcast.

On June 14, 2005, the trial judge issued a memorandum opinion denying Doe’s motion for a protective order. The Superior Court judge adopted a “good faith” standard for determining when a defamation plaintiff could compel the disclosure of the identity of an anonymous plaintiff. Under the good faith standard, the Superior Court required the Cahills to establish: (1) that they had a legitimate, good faith basis upon which to bring the underlying claim; (2) that the identifying information sought was directly and materially related to their claim; and (3) that the information could not be obtained from any other source. Applying this standard, the Superior Court held that the Cahills could obtain Doe’s identity from Comcast. Doe filed an interlocutory appeal, which we accepted on June 28, 2005.

The internet is a unique democratizing medium unlike anything that has come before. The advent of the internet dramatically changed the nature of public discourse by allowing more and diverse people to engage in public debate.

Internet speech is often anonymous. “Many participants in cyberspace discussions employ pseudonymous identities, and, even when a speaker chooses to reveal her real name, she may still be anonymous for all practical purposes.”

It is clear that speech over the internet is entitled to First Amendment protection. This protection extends to anonymous internet speech. Anonymous internet speech in blogs or chat rooms in some instances can become the modern equivalent of political pamphleteering. As the United States Supreme Court recently noted, “anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and dissent.” The United States Supreme Court continued, “[t]he right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse.”

38 47 U.S.C. 551(c)(2) requires a court order to a cable ISP and notice to the ISP subscriber before an ISP can disclose the identity of its subscriber to a third party.
It also is clear that the First Amendment does not protect defamatory speech. “[I]t is well understood that the right of free speech is not absolute at all times and under all circumstances.” Certain classes of speech, including defamatory and libelous speech, are entitled to no Constitutional protection. . . . Accordingly, we must adopt a standard that appropriately balances one person’s right to speak anonymously against another person’s right to protect his reputation. . . .

In this case, this Court is called upon to adopt a standard for trial courts to apply when faced with a public figure plaintiff’s discovery request that seeks to unmask the identity of an anonymous defendant who has posted allegedly defamatory material on the internet. Before this Court is an entire spectrum of “standards” that could be required, ranging (in ascending order) from a good faith basis to assert a claim, to pleading sufficient facts to survive a motion to dismiss, to a showing of *prima facie* evidence sufficient to withstand a motion for summary judgment, and beyond that, hurdles even more stringent. The Cahills urge this Court to adopt the good faith standard applied by the Superior Court. We decline to do so. Instead we hold that a defamation plaintiff must satisfy a “summary judgment” standard before obtaining the identity of an anonymous defendant.

We are concerned that setting the standard too low will chill potential posters from exercising their First Amendment right to speak anonymously. The possibility of losing anonymity in a future lawsuit could intimidate anonymous posters into self-censoring their comments or simply not commenting at all. A defamation plaintiff, particularly a public figure, obtains a very important form of relief by unmasking the identity of his anonymous critics. The revelation of identity of an anonymous speaker “may subject [that speaker] to ostracism for expressing unpopular ideas, invite retaliation from those who oppose her ideas or from those whom she criticizes, or simply give unwanted exposure to her mental processes.” Plaintiffs can often initially plead sufficient facts to meet the good faith test applied by the Superior Court, even if the defamation claim is not very strong, or worse, if they do not intend to pursue the defamation action to a final decision. After obtaining the identity of an anonymous critic through the compulsory discovery process, a defamation plaintiff who either loses on the merits or fails to pursue a lawsuit is still free to engage in extra-judicial self-help remedies; more bluntly, the plaintiff can simply seek revenge or retribution.

Indeed, there is reason to believe that many defamation plaintiffs bring suit merely to unmask the identities of anonymous critics. As one commentator has noted, “[t]he sudden surge in John Doe suits stems from the fact that many defamation actions are not really about money.” “The goals of this new breed of libel action are largely symbolic, the primary goal being to silence John Doe and others like him.” This “sue first, ask questions later” approach, coupled with a standard only minimally protective of the anonymity of defendants, will discourage debate on important issues of public concern as more and more anonymous posters censor their online statements in response to the likelihood of being unmasked. . . .

Long-settled doctrine governs this Court’s review of dismissals under Rule 12(b)(6). Under that doctrine, the threshold for the showing a plaintiff must make to survive a motion to dismiss is low. Delaware is a notice pleading jurisdiction. Thus, for a complaint to survive a motion to dismiss, it need only give “general notice of the claim asserted.” A court can dismiss for failure to state a claim on which relief can be granted.
On a motion to dismiss, a court’s review is limited to the well-pleaded allegations in the complaint. An allegation, “though vague or lacking in detail” can still be well-pleaded so long as it puts the opposing party on notice of the claim brought against it. Finally, in ruling on a motion to dismiss under Rule 12(b)(6), a trial court must draw all reasonable factual inferences in favor of the party opposing the motion.

Even silly or trivial libel claims can easily survive a motion to dismiss where the plaintiff pleads facts that put the defendant on notice of his claim, however vague or lacking in detail these allegations may be. Clearly then, if the stricter motion to dismiss standard is incapable of screening silly or trivial defamation suits, then the even less stringent good faith standard is less capable of doing so.

A summary judgment proceeding can dispense with weak or even “silly” libel cases before trial (but even then only after significant expense and anxiety to the parties). Applying a summary judgment standard to a public figure defamation plaintiff’s discovery request to obtain an anonymous defendant’s identity will more appropriately protect against the chilling effect on anonymous First Amendment internet speech that can arise when plaintiffs bring trivial defamation lawsuits primarily to harass or to unmask their critics.

We conclude that the summary judgment standard is the appropriate test by which to strike the balance between a defamation plaintiff’s right to protect his reputation and a defendant’s right to exercise free speech anonymously. We accordingly hold that before a defamation plaintiff can obtain the identity of an anonymous defendant through the compulsory discovery process he must support his defamation claim with facts sufficient to defeat a summary judgment motion.

To the extent reasonably practicable under the circumstances, the plaintiff must undertake efforts to notify the anonymous poster that he is the subject of a subpoena or application for order of disclosure. The plaintiff must also withhold action to afford the anonymous defendant a reasonable opportunity to file and serve opposition to the discovery request. Moreover, when a case arises in the internet context, the plaintiff must post a message notifying the anonymous defendant of the plaintiff’s discovery request on the same message board where the allegedly defamatory statement was originally posted.

Although a good faith or motion to dismiss standard sets the bar too low to protect a defendant’s First Amendment right to speak anonymously on the internet, a summary judgment standard does not correspondingly set the bar too high for a defamation plaintiff seeking redress for reputational harm to obtain relief.

To obtain discovery of an anonymous defendant’s identity under the summary judgment standard, a defamation plaintiff “must submit sufficient evidence to establish a prima facie case for each essential element of the claim in question.” In other words, the defamation plaintiff, as the party bearing the burden of proof at trial, must introduce evidence creating a genuine issue of material fact for all elements of a defamation claim within the plaintiff’s control.

Under Delaware law, a public figure defamation plaintiff in a libel case must plead and ultimately prove that: 1) the defendant made a defamatory statement; 2) concerning the plaintiff; 3) the statement was published; and 4) a third party would
understand the character of the communication as defamatory. In addition, the public figure defamation plaintiff must plead and prove that 5) the statement is false and 6) that the defendant made the statement with actual malice. Finally, “[p]roof of damages proximately caused by a publication deemed libelous need not be shown in order for a defamed plaintiff to recover nominal or compensatory damages.” . . .

We are mindful that public figures in a defamation case must prove that the defendant made the statements with actual malice. Without discovery of the defendant’s identity, satisfying this element may be difficult, if not impossible. Consequently, we do NOT hold that the public figure defamation plaintiff is required to produce evidence on this element of the claim. We hold only that a public figure plaintiff must plead the first five elements and offer *prima facie* proof on each of the five elements to create a genuine issue of material fact requiring trial. In other words, a public figure defamation plaintiff must only plead and prove facts with regard to elements of the claim that are within his control. . . .

Having adopted a summary judgment standard, we now apply it to the facts of this case. . . .

In deciding whether or not a statement is defamatory we determine, “first, whether alleged defamatory statements are expressions of fact or protected expressions of opinion; and [second], whether the challenged statements are capable of a defamatory meaning.” . . .

Applying a good faith standard, the trial judge concluded, “it is enough to meet the ‘good faith’ standard that the Cahills articulate a legitimate basis for claiming defamation in the context of their particular circumstances.” He continued “[g]iven that Mr. Cahill is a married man, [Doe’s] statement referring to him as “Gahill” might reasonably be interpreted as indicating that Mr. Cahill has engaged in an extra-marital same-sex affair. Such a statement may form the basis of an actionable defamation claim.” We disagree. Using a “G” instead of a “C” as the first letter of Cahill’s name is just as likely to be a typographical error as an intended misguided insult. Under the summary judgment standard, no reasonable person would interpret this statement to indicate that Cahill had an extra-marital same-sex affair. With respect to Doe’s other statements, the trial judge noted:

Again, the context in which the statements were made is probative. [Doe’s] statements might give the reader the impression that [Doe] has personal knowledge that Mr. Cahill’s mental condition is deteriorating and that he is becoming “paranoid.” Given that Mr. Cahill is a member of the Smyrna Town Council, an elected position of public trust, the impression that he is suffering from diminished mental capacity might be deemed capable of causing harm to his reputation, particularly when disseminated over the internet for all of his constituents to read.

We agree that the context in which the statements were made is probative, but reach the opposite conclusion. Given the context, no reasonable person could have interpreted these statements as being anything other than opinion. The guidelines at the top of the blog specifically state that the forum is dedicated to *opinions* about issues in Smyrna. . . .

At least one reader of the blog quickly reached the conclusion that Doe’s comments were no more than unfounded and unconvincing opinion. Given the context of the statement and the normally (and inherently) unreliable nature of assertions posted in
chat rooms and on blogs, this is the only supportable conclusion. Read in the context of an internet blog, these statements did not imply any assertions of underlying objective facts. Accordingly, we hold that as a matter of law a reasonable person would not interpret Doe’s statements as stating facts about Cahill. The statements are, therefore, incapable of a defamatory meaning. Because Cahill has failed to plead an essential element of his claim, he ipso facto cannot produce prima facie proof of that first element of a libel claim, and thus, cannot satisfy the summary judgment standard we announce today. Doe’s statements simply are not sufficient to give rise to a prima facie case for defamation liability. . . .

NOTES & QUESTIONS

p. 489 – Replace note 1 with the following:

1. The Standard for Unmasking an Anonymous Speaker. Do you agree with the court in Doe v. Cahill that the summary judgment standard as opposed to the good faith standard is the appropriate one for unmasking an anonymous speaker? What reasons could plaintiffs give as to why a summary judgment standard would be too high? Or, on the other hand, is a summary judgment standard too low?

p. 489—Add new note 2, renumber subsequent notes. Doe v. 2TheMart will now be covered in this note:

2. The Identities of Third Parties to the Litigation. In Doe v. 2TheMart.com, Inc. 140 F.Supp.2d 1088 (W.D. Wash. 2001), shareholders of 2TheMart.com, Inc. brought a derivative class action against the corporation. The company, in preparing its defense, subpoenaed the identity of twenty-three anonymous speakers who posted messages on an online message board. These postings were very critical of 2TheMart. One of the anonymous speakers challenged the subpoena. The court concluded:

The free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously. If Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights. Therefore, discovery requests seeking to identify anonymous Internet users must be subjected to careful scrutiny by the courts. . . .

In the context of a civil subpoena issued pursuant to Fed. R. Civ. P. 45, this Court must determine when and under what circumstances a civil litigant will be permitted to obtain the identity of persons who have exercised their First Amendment right to speak anonymously. There is little in the way of persuasive authority to assist this Court. However, courts that have addressed related issues have used balancing tests to decide when to protect an individual’s First Amendment rights. . . .

The standard for disclosing the identity of a non-party witness must be higher than that [required for a party to the litigation]. . . . When the anonymous Internet user is not a party to the case, the litigation can go forward without the disclosure of their identity. Therefore, non-party disclosure is only appropriate in the exceptional case where the compelling need for the discovery sought outweighs the First Amendment rights of the anonymous speaker.

Accordingly, this Court adopts the following standard for evaluating a civil subpoena that seeks the identity of an anonymous Internet user who is not a party to the underlying litigation. The Court will consider four factors in determining whether the subpoena should issue. These are
whether: (1) the subpoena seeking the information was issued in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source. . . .

Only when the identifying information is needed to advance core claims or defenses can it be sufficiently material to compromise First Amendment rights. If the information relates only to a secondary claim or to one of numerous affirmative defenses, then the primary substance of the case can go forward without disturbing the First Amendment rights of the anonymous Internet users.
The information sought by TMRT does not relate to a core defense. Here, the information relates to only one of twenty-seven affirmative defenses raised by the defendant, the defense that “no act or omission of any of the Defendants was the cause in fact or the proximate cause of any injury or damage to the plaintiffs.” . . . .

[Moreover,] TMRT has failed to demonstrate that the identity of the Internet users is directly and materially relevant to a core defense. These Internet users are not parties to the case and have not been named as defendants as to any claim, cross-claim or third-party claim. . . .

3. ANONYMOUS READING AND RECEIVING OF IDEAS

p. 497 – Add new note after note 5; renumber existing note 6:

6. The First Amendment as Criminal Procedure. Daniel Solove contends that the First Amendment should be employed to protect against many forms of government searches and surveillance:

The First Amendment is usually taught separately from the Fourth and Fifth Amendments, and judicial decisions on criminal procedure only occasionally mention the First Amendment. I contend in this Article, however, that the First Amendment must be considered alongside the Fourth and Fifth Amendments as a source of criminal procedure.

First Amendment activities are implicated by a wide array of law enforcement data-gathering activities. Government information gathering about computer and Internet use, for example, can intrude on a significant amount of First Amendment activity. Searching or seizing a computer can reveal personal and political writings. Obtaining e-mail can provide extensive information about correspondence and associations. Similarly, ISP records often contain information about speech, as they can link people to their anonymous communications. AOL, for example, receives about a thousand requests per month for use of its customer records in criminal cases.

The government can also use subpoenas to gather information about First Amendment activities such as book reading and personal writing. . . .

Freedom of association can be implicated when the government monitors or attempts to infiltrate political groups. Freedom of the press can be compromised when the government subpoenas journalists to provide the identities of confidential sources, or when the police search the offices or computers of media entities. And with blogs supplementing the traditional media, searches of individual homes and computers might also implicate journalistic activities.

Solove contends that there is a doctrinal foundation for First Amendment protection against government information gathering. If the First Amendment were to apply to certain government law enforcement activities, what level of protections would it provide? Solove argues:

Even if an instance of government information gathering triggers First Amendment protection,
collection of the data will not necessarily be prohibited. Rather, the First Amendment will require the government to demonstrate (1) a significant interest in gathering the information and (2) that the manner of collection is narrowly tailored to achieving that interest. As I will discuss in this Section, the use of a warrant supported by probable cause will, in most cases, suffice to satisfy the narrow tailoring requirement. In other words, in cases where the First Amendment applies, it often will require procedures similar to those required by the Fourth Amendment.  

Solove also posits that the First Amendment would be enforced by way of an exclusionary rule. To what extent does the First Amendment apply to government law enforcement activities? Should the First Amendment require similar protections to those of the Fourth Amendment or greater protections as in *Tattered Cover*?

p. 498 – Add the following at the end of existing note 6:

Consider Marc Blitz:

Courts and scholars do not need to be convinced that the First Amendment gives individuals a right to receive the ideas expressed by others: provocative speeches and public protests are valuable for a democracy and its citizens not in and of themselves, but rather because they provide the raw material for other less visible deliberations that occur later on, in libraries, private living rooms, and in people’s own minds. The First Amendment thus protects both the public act that sparks such debate and the informal conversations and ruminations that keep it alive and allow it to radiate into the corners of everyday life.

But it has been my argument in this article that the First Amendment right to receive information also does something more. It not only protects paths for citizens’ communication of ideas, but also the somewhat different paths that information-seekers use to track down ideas that are lying dormant. Crucial to this second activity is the protection of public libraries. As the British liberal statesman, Herbert Samuel, once said: “A library is thought in cold storage.” It is a place where ideas are frozen and preserved for information-seekers-put in the form of what George Simmel called “objectified knowledge”—so that they remain available during the many years it might take an individual find them (along with thousands or millions of other cultural and intellectual sources).

---


SUMMARY OF ADDITIONS TO CHAPTER

- In A.1 (public records and court records), we added a new case to introduce the section – Doe v. Shakur.

- In B.3(c) (government data mining), we added an excerpt from United States v. Ellison, a case involving whether searching for information in a computer database constitutes a Fourth Amendment violation.

A. PUBLIC ACCESS TO GOVERNMENT RECORDS

1. PUBLIC RECORDS AND COURT RECORDS

p. 526 – Add the following at the end of Section 1 after the excerpt of Solove’s Access and Aggregation article:

**DOE V. SHAKUR**

164 F.R.D. 359 (S.D.N.Y. 1996)

CHIN, J. This diversity action raises the difficult question of whether the victim of a sexual assault may prosecute a civil suit for damages under a pseudonym. Plaintiff has brought this action charging that defendants Tupac A. Shakur and Charles L. Fuller sexually assaulted her on November 18, 1993. On December 1, 1994, a jury trial in Supreme Court, New York County, found Shakur and Fuller guilty of sexual abuse and not guilty of sodomy, attempted sodomy and weapons violations. They were sentenced on February 7, 1995 and an appeal is pending.

This civil suit was filed approximately two weeks after Shakur and Fuller were sentenced. The complaint seeks $10 million in compensatory damages and $50 million in punitive damages. Before filing her complaint, plaintiff obtained an order *ex parte* from Judge Sprizzo, sitting as Part I judge, sealing the complaint and permitting plaintiff to file a substitute complaint using a pseudonym in place of her real name. Neither defendant filed a timely answer and thus the Clerk of the Court entered a default.

Shakur has moved to vacate the entry of default. In his motion papers, which have not yet been filed with the Clerk of the Court but which have been served on plaintiff, Shakur identifies plaintiff by her real name. Shakur justifies his use of plaintiff’s name by noting that Judge Sprizzo’s order allowing plaintiff to file her complaint using a pseudonym was signed after an *ex parte* appearance and merely sealed the complaint. That order did not provide that this entire proceeding was to be
conducted under seal. In response, plaintiff claims that Judge Sprizzo’s order requires all papers filed with the Court to use plaintiff’s pseudonym. In the alternative, plaintiff requests that I issue such an order now.

As a threshold matter, it is plain from the face of Judge Sprizzo’s order that he did not decide the issue now before me. Judge Sprizzo’s order merely allowed plaintiff to file the complaint under seal. Judge Sprizzo did not order that all documents filed in this case be sealed. Nor did Judge Sprizzo hold that plaintiff could prosecute the entire lawsuit under a pseudonym. Nor do I believe that Judge Sprizzo, sitting as Part I judge on the basis of an ex parte application, intended to foreclose defendants from being heard on the issue.

Rule 10(a) of the Federal Rules of Civil Procedure provides that a complaint shall state the names of all the parties. The intention of this rule is to apprise parties of who their opponents are and to protect the public’s legitimate interest in knowing the facts at issue in court proceedings. Nevertheless, in some circumstances a party may commence a suit using a fictitious name.

It is within a court’s discretion to allow a plaintiff to proceed anonymously. Doe v. Bell Atlantic Business Sys. Servs., Inc., 162 F.R.D. 418, 420 (D.Mass.1995). In exercising its discretion, a court should consider certain factors in determining whether plaintiffs may proceed anonymously. These factors include (1) whether the plaintiff is challenging governmental activity; (2) whether the plaintiff would be required to disclose information of the utmost intimacy; (3) whether the plaintiff would be compelled to admit his or her intention to engage in illegal conduct, thereby risking criminal prosecution; (4) whether the plaintiff would risk suffering injury if identified; and (5) whether the party defending against a suit brought under a pseudonym would be prejudiced.

In considering these and other factors, a court must engage in a balancing process. As the Eleventh Circuit has held,

The ultimate test for permitting a plaintiff to proceed anonymously is whether the plaintiff has a substantial privacy right which outweighs the ‘customary and constitutionally-embedded presumption of openness in judicial proceedings.’ It is the exceptional case in which a plaintiff may proceed under a fictitious name.

Frank, 951 F.2d at 323 (citing Doe v. Stegall, 653 F.2d 180, 186 (5th Cir.1981)).

The present case is a difficult one. If the allegations of the complaint are true, plaintiff was the victim of a brutal sexual assault. Quite understandably, she does not want to be publicly identified and she has very legitimate privacy concerns. On balance, however, these concerns are outweighed by the following considerations.

First, plaintiff has chosen to bring this lawsuit. She has made serious charges and has put her credibility in issue. Fairness requires that she be prepared to stand behind her charges publicly.

Second, this is a civil suit for damages, where plaintiff is seeking to vindicate primarily her own interests. This is not a criminal case where rape shield laws might provide some anonymity to encourage victims to testify to vindicate the public’s interest in enforcement of our laws. See id. (rape shield laws “apply to situations where the government chooses to prosecute a case, and offer[ ] anonymity to a victim who does not have a choice in or control over the prosecution”). Indeed, the public’s interest in
bringing defendants to justice for breaking the law—assuming that they did—is being vindicated in the criminal proceedings.

Third, Shakur has been publicly accused. If plaintiff were permitted to prosecute this case anonymously, Shakur would be placed at a serious disadvantage, for he would be required to defend himself publicly while plaintiff could make her accusations from behind a cloak of anonymity.

Finally, the public has a right of access to the courts. Indeed, “lawsuits are public events and the public has a legitimate interest in knowing the facts involved in them. Among those facts is the identity of the parties.” . . . .

Plaintiff argues that Shakur’s notoriety will likely cause this case to attract significant media attention, and she contends that disclosure of her name will cause her to be “publicly humiliated and embarrassed.” Such claims of public humiliation and embarrassment, however, are not sufficient grounds for allowing a plaintiff in a civil suit to proceed anonymously, as the cases cited above demonstrate. Moreover, plaintiff has conceded that the press has known her name for some time. Indeed, plaintiff makes it clear that the press has been aware of both her residence and her place of employment. Hence, her identity is not unknown.

Plaintiff’s allegation that she has been subjected to death threats would provide a legitimate basis for allowing her to proceed anonymously. Plaintiff has not, however, provided any details, nor has she explained how or why the use of her real name in court papers would lead to harm, since those who presumably would have any animosity toward her already know her true identity. Thus, plaintiff simply has not shown that she is entitled to proceed under a pseudonym in this action.

It may be, as plaintiff suggests, that victims of sexual assault will be deterred from seeking relief through civil suits if they are not permitted to proceed under a pseudonym. That would be an unfortunate result. For the reasons discussed above, however, plaintiff and others like her must seek vindication of their rights publicly.

**NOTES & QUESTIONS**

1. *Pseudonymous Litigation.* *Doe v. Shakur* involved a party’s request to proceed under a pseudonym. The standard for allowing a party to proceed with a fictitious name gives significant room for judicial discretion. Consider *Doe v. Blue Cross & Blue Shield United of Wisconsin*, 112 F.3d 869 (7th Cir. 1997):

   The plaintiff is proceeding under a fictitious name because of fear that the litigation might result in the disclosure of his psychiatric records. The motion to proceed in this way was not opposed, and the district judge granted it without comment. The judge’s action was entirely understandable given the absence of objection and the sensitivity of psychiatric records, but we would be remiss if we failed to point out that the privilege of suing or defending under a fictitious name should not be granted automatically even if the opposing party does not object. The use of fictitious names is disfavored, and the judge has an independent duty to determine whether exceptional circumstances justify such a departure from the normal method of proceeding in federal courts. See *United States v. Microsoft Corp.*, 56 F.3d 1448, 1463-64 (D.C.Cir.1995) (per curiam), and cases cited there,
and our recent dictum in *K.F.P. v. Dane County*, 110 F.3d 516, 518-19 (7th Cir.1997). Rule 10(a) of the Federal Rules of Civil Procedure, in providing that the complaint shall give the names of all the parties to the suit (and our plaintiff’s name is *not* “John Doe”), instantiates the principle that judicial proceedings, civil as well as criminal, are to be conducted in public. Identifying the parties to the proceeding is an important dimension of publicness. The people have a right to know who is using their courts.

There are exceptions. Records or parts of records are sometimes sealed for good reasons, including the protection of state secrets, trade secrets, and informers; and fictitious names are allowed when necessary to protect the privacy of children, rape victims, and other particularly vulnerable parties or witnesses. But the fact that a case involves a medical issue is not a sufficient reason for allowing the use of a fictitious name, even though many people are understandably secretive about their medical problems. “John Doe” suffers, or at least from 1989 to 1991 suffered, from a psychiatric disorder-obsessive-compulsive syndrome. This is a common enough disorder-some would say that most lawyers and judges suffer from it to a degree-and not such a badge of infamy or humiliation in the modern world that its presence should be an automatic ground for concealing the identity of a party to a federal suit. To make it such would be to propagate the view that mental illness is shameful. Should “John Doe”’s psychiatric records contain material that would be highly embarrassing to the average person yet somehow pertinent to this suit and so an appropriate part of the judicial record, the judge could require that this material be placed under seal.

When is it appropriate for a judge to allow a party to proceed under a pseudonym? Does the test give too much discretion to judges to make this determination? If so, how would you draft a rule that provides a more definitive approach to this issue?

The following note incorporates the last paragraph at the bottom of p. 542, which is moved to here:

2. **Protective Orders.** Federal Rule of Civil Procedure 26(c) provides that judges may, “for good cause shown,” issue protective orders where disclosure of information gleaned in discovery might cause a party “annoyance, embarrassment, oppression, or undue burden or expense.” Most states have similar protective order provisions. There is a presumption in favor of access, and the party seeking the protective order must overcome this presumption. Courts will issue a protective order when a party’s interest in privacy outweighs the public interest in disclosure.41 Although the standard for obtaining a protective order is easier to satisfy than the standard for proceeding under a pseudonym, the thumb on the scale is on the side of public access. Is there too much discretion in granting protective orders?

---

3. Categorical Exclusion of Personal Information in Court Records. Under some court practices, certain information is categorically excluded from court records. As Natalie Gomez-Velez notes:

The list of data elements categorically excluded from case records varies from state to state, depending to some extent on the degree to which case records are being made available and the extent to which a particular state precludes public access to certain categories of cases and information. . . .

To a great extent, the federal courts, New York, Indiana, and courts in other states that exclude whole classes of sensitive cases like matrimonial, adoption, juvenile, and family law cases from public access, have fewer problems to solve than courts that permit public access to these kinds of cases.42

3. THE USE OF GOVERNMENT DATABASES
(c) Government Data Mining

p. 617 – Add the following after note 6:

UNITED STATES v. ELLISON
462 F.3d 557 (6th Cir. 2006)

GIBBONS, J. . . . The central issue in this case is whether the Fourth Amendment is implicated when a police officer investigates an automobile license plate number using a law enforcement computer database. While on routine patrol, Officer Mark Keeley of the Farmington Hills (Michigan) Police Department pulled into a two-lane service drive adjacent to a shopping center. Keeley testified that a white van, with a male driver inside, was idling in the lane closest to the stores, in an area marked with “Fire Lane” and “No Parking” signs. Keeley did not issue the van a citation for being illegally parked, nor did he request that the driver move the van. Rather, he moved into a parking spot to observe the van and entered the vehicle’s license plate number into his patrol car’s Law Enforcement Information Network (“LEIN”) computer. The LEIN search revealed that the vehicle was registered to Curtis Ellison, who had an outstanding felony warrant. Following standard procedure, Keeley radioed for back-up and continued observing the van. After two minutes, another male got into the van, and it drove away. Officer Keeley followed the van until his back-up was nearby, and then activated his lights and stopped the van.

Officer Keeley approached the driver’s-side window as his back-up arrived. He advised the driver that he was being stopped for parking in a fire lane and asked for license, registration and proof of insurance. The driver, identified as Edward Coleman, stated that he had only stopped in front of the store to wait for the passenger. At this time the passenger stated that he was the registered owner of the vehicle. Keeley verified the passenger’s identity as Curtis Ellison and moved to the passenger side of the van. Keeley notified Ellison that he was being arrested on the outstanding warrant. Ellison stepped out of the van, and during the routine safety pat-down, two firearms were

found. Coleman was released with a warning about parking in a fire lane.

Ellison was indicted for being a felon in possession of a firearm in violation of 18 U.S.C. § 922(g). Prior to trial, he made a timely motion to suppress the firearm as the fruit of an illegal search. After holding a hearing, the district court made a factual finding that the van was not parked illegally, and thus, the officer did not have probable cause to run the LEIN check of Ellison’s license plate. The court issued a Memorandum Opinion and Order granting the motion to suppress under the “fruit of the poisonous tree” doctrine. . . .

The government argues on appeal that Ellison had no reasonable expectation of privacy in the information contained on his license plate, and thus, no probable cause was required for Officer Keeley to run the LEIN check. . . .

Although the district court did not expressly state that Ellison had a reasonable expectation of privacy in the information contained on his license plate, such a conclusion was necessarily implied by the court’s ruling that a Fourth Amendment violation occurred. Thus, the district court could only find that the LEIN search violated the Fourth Amendment if it first concluded that Ellison had a ‘constitutionally protected reasonable expectation of privacy’ in his license plate number. . . .

A tenet of constitutional jurisprudence is that the Fourth Amendment protects only what an individual seeks to keep private. Katz, 389 U.S. at 351-52. “What a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection.” It is also settled that “objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure.” . . .

No argument can be made that a motorist seeks to keep the information on his license plate private. The very purpose of a license plate number, like that of a Vehicle Identification Number, is to provide identifying information to law enforcement officials and others. . . .

The dissent implies that even if an individual has no expectation of privacy in a license plate number, a privacy interest is somehow created by the entry of this information into a law-enforcement computer database. This argument flies in the face of established Fourth Amendment doctrine. First, despite the dissent’s concerns over the information available in a LEIN search, Ellison had no privacy interest in the information retrieved by Officer Keely. The obvious purpose of maintaining law enforcement databases is to make information, such as the existence of outstanding warrants, readily available to officers carrying out legitimate law enforcement duties. The dissent fails to state how using a license plate number-in which there is no expectation of privacy-to retrieve other non-private information somehow creates a “search” for the purposes of the Fourth Amendment. . . . This is not a case where the police used a technology not available to the public to discover evidence that could not otherwise be obtained without “intrusion into a constitutionally-protected area.” Kyllo v. United States, 533 U.S. 27, 34-35 (2001) (holding that the use of thermal-imaging technology to detect heat inside a private home violates the Fourth Amendment). The technology used in this case does not allow officers to access any previously-unobtainable information; it simply allows them to access information more quickly. As the information was obtained without intruding upon a constitutionally-protected area, there was no “search” for Fourth Amendment purposes. . . .
MOORE, J. DISSENTING. . . . The majority rests its conclusion that the Fourth Amendment was not implicated by the LEIN search on the relatively uncontroversial fact that the operator of a vehicle has no privacy interest in the particular combination of letters and numerals that make up his license-plate number, but pays short shrift to the crucial issue of how the license-plate information is used. . . . This approach misses the crux of the issue before the court: even if there is no privacy interest in the license-plate number per se, can the police, without any measure of heightened suspicion or other constraint on their discretion, conduct a search using the license-plate number to access information about the vehicle and its operator that may not otherwise be public or accessible by the police without heightened suspicion? . . .

The use of a computer database to acquire information about drivers through their license-plate numbers without any heightened suspicion is in tension with many of the Fourth Amendment concerns expressed in Delaware v. Prouse, 440 U.S. 648, 655-63 (1979). In Prouse, the Supreme Court held that an officer may not stop a vehicle to check the operator’s license and registration without “at least articulable and reasonable suspicion that a motorist is unlicensed or that an automobile is not registered, or that either the vehicle or an occupant is otherwise subject to seizure for violation of law,” despite the fact that the state requires drivers to be licensed and vehicles to be registered. The Court stated that the Fourth Amendment aims “to safeguard the privacy and security of individuals against arbitrary invasions.... Thus, the permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual’s Fourth Amendment interests against its promotion of legitimate governmental interests.” The Court then explained the constitutional concerns that flow from the unbridled discretion associated with permitting random searches of drivers’ information:

To insist neither upon an appropriate factual basis for suspicion directed at a particular automobile nor upon some other substantial and objective standard or rule to govern the exercise of discretion “would invite intrusions upon constitutionally guaranteed rights based on nothing more substantial than inarticulate hunches. . . .” Terry v. Ohio, 392 U.S. [1], at 22 [1968] . . . . When there is not probable cause to believe that a driver is violating any one of the multitude of applicable traffic and equipment regulations-or other articulable basis amounting to reasonable suspicion that the driver is unlicensed or his vehicle unregistered—we cannot conceive of any legitimate basis upon which a patrolman could decide that stopping a particular driver for a spot check would be more productive than stopping any other driver. This kind of standardless and unconstrained discretion is the evil the Court has discerned when in previous cases it has insisted that the discretion of the official in the field be circumscribed, at least to some extent. . . .

Although the license-plate search at issue here is arguably less invasive than a license-and-registration check, the constitutional concerns regarding abuse of discretion do not disappear simply because drivers are not stopped to conduct the license-plate search. First, a search can implicate the Fourth Amendment even when the individual does not know that she is being searched. Second, the balancing of Fourth Amendment interests also requires consideration of “psychological intrusion[s] visited upon” the individuals searched in assessing the extent of intrusion that a particular police practice imposes. See Prouse, 440 U.S. at 657 The psychological invasion that results from knowing that one’s personal information is subject to search by the police, for no reason, at any time one is driving a car is undoubtedly grave.

Because the government incorrectly limits its Fourth Amendment analysis to the
plain view of the license plate without exploring the constitutional implications of the subsequent LEIN search, it does not provide any explanation as to the governmental interests promoted by license-plate searches.

In addition, the possibility and the reality of errors in the computer databases accessed by MDT systems lead to great concern regarding the potential for license-plate searches to result in unwarranted intrusions into privacy in the form of stops made purely on the basis of incorrect information.

NOTES & QUESTIONS

The following note is taken from note 5 on p. 616. It should be read and discussed after United States v. Ellison. The note is reproduced below:

1. The Fourth Amendment and Government Data Mining. Does the Fourth Amendment provide any limits on government data mining? Lee Tein argues that it does:

   The use of patterns discovered through data mining raises . . . particularity issues. Imagine a database of a million people and a hypothesis that those who meet certain criteria are highly likely to be terrorists. But you don’t know whether any of these million people actually do meet these criteria; if you did, you wouldn’t need to run the search. The basic problem is lack of particularized suspicion; data about these persons would be “searched” without any reason to believe either that the database contains evidence of terrorist activity or that any person “in” the database is a terrorist. . . .

   When the government engages in data mining, it often analyzes information that it already possesses. Is this a search? If the government has information about a person in its records and analyzes it, does this trigger the Fourth Amendment?

---

CHAPTER 7:
PRIVACY, BUSINESS RECORDS, AND
FINANCIAL INFORMATION

SUMMARY OF ADDITIONS TO CHAPTER

- In B.5.b (Computer Fraud and Abuse Act), we added a new case, *Creative Computing*.

- In B.5.c (Video Privacy Protection Act), we added a case, *Daniel v. Cantell*, that comes to a different result than *Dirkes v. Borough of Runnemede*, concerning whether the Video Privacy Protection Act extends to the behavior of actors other than a “video tape service provider.”

- In D.4 (Database Companies, Security Breaches, and Identity Theft), we added new material about breach notification statutes.

- In G.1(a) (Administrative and Grand Jury Subpoenas), we added a new case, Gonzales v. Google, which looks at government access to queries sent to a search engine.

- In H.2 (private enforcement of privacy policies: contract remedies), we added more notes following *In re Northwest Airlines Privacy Litigation*, including a brief excerpt from *In re Jet Blue Airways Corp. Privacy Litigation*.

B. REGULATING BUSINESS RECORDS AND DATABASES

5. STATUTORY PROTECTIONS

(b) Computer Fraud and Abuse Act

p. 658 – Replace Chance v. Avenue A with the following case:

**Creative Computing v. Getloaded.com LLC**

386 F.3d 930 (9th Cir. 2004)

**KLEINFELD, J.** Truck drivers and trucking companies try to avoid dead heading. “Deadheading” means having to drive a truck, ordinarily on a return trip, without a revenue-producing load. If the truck is moving, truck drivers and their companies want it to be carrying revenue-producing freight. In the past, truckers and shippers used blackboards to match up trips and loads. Eventually television screens were used instead of blackboards, but the matching was still inefficient. Better information on where the trucks and the loads are-and quick, easy access to that information-benefits shippers, carriers, and consumers.

Creative Computing developed a successful Internet site, truckstop.com, which it calls “The Internet Truckstop,” to match loads with trucks. The site is very easy to use.
It has a feature called “radius search” that lets a truck driver in, say, Middletown, Connecticut, with some space in his truck, find within seconds all available loads in whatever mileage radius he likes (and of course lets a shipper post a load so that a trucker with space can find it). The site was created so early in Internet history and worked so well that it came to dominate the load-board industry.

Getloaded decided to compete, but not honestly. After Getloaded set up a load-matching site, it wanted to get a bigger piece of Creative’s market. Creative wanted to prevent that, so it prohibited access to its site by competing load-matching services. The Getloaded officers thought trucking companies would probably use the same login names and passwords on truckstop.com as they did on getloaded.com. Getloaded’s president, Patrick Hull, used the login name and password of a Getloaded subscriber, in effect impersonating the trucking company, to sneak into truckstop.com. Getloaded’s vice-president, Ken Hammond, accomplished the same thing by registering a defunct company, RFT Trucking, as a truckstop.com subscriber. These tricks enabled them to see all of the information available to Creative’s bona fide customers.

Getloaded’s officers also hacked into the code Creative used to operate its website. Microsoft had distributed a patch to prevent a hack it had discovered, but Creative Computing had not yet installed the patch on truckstop.com. Getloaded’s president and vice-president hacked into Creative Computing’s website through the back door that this patch would have locked. Once in, they examined the source code for the tremendously valuable radius-search feature.

Getloaded argues that no action could lie under the Computer Fraud and Abuse Act because it requires a $5,000 floor for damages from each unauthorized access, and that Creative Computing submitted no evidence that would enable a jury to find that the floor was reached on any single unauthorized access.

The briefs dispute which version of the statute we should apply—the one in effect when Getloaded committed the wrongs, or the one in effect when the case went to trial (which is still in effect). The old version of the statute made an exception to the fraudulent access provision if “the value of such use [unauthorized access to a protected computer] is not more than $5,000 in any 1-year period.” The new version, in effect now and during trial, says “loss ... during any 1-year period ... aggregating at least $5,000 in value.” These provisions are materially identical.

The old version of the statute defined “damage” as “any impairment to the integrity or availability of data, a program, a system, or information” that caused the loss of at least $5,000. It had no separate definition of “loss.” The new version defines “damage” the same way, but adds a definition of loss. “Loss” is defined in the new version as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data ... and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.”

44 18 U.S.C. § 1030(a)(4) (2001) (“[Whoever] knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.”).
45 18 U.S.C. § 1030(a)(5)(B)(i) (“Whoever caused] loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value.”).
For purposes of this case, we need not decide which version of the Act applies, because Getloaded loses either way. Neither version of the statute supports a construction that would require proof of $5,000 of damage or loss from a single unauthorized access. The syntax makes it clear that in both versions, the $5,000 floor applies to how much damage or loss there is to the victim over a one-year period, not from a particular intrusion. Getloaded argues that “impairment” is singular, so the floor has to be met by a single intrusion. The premise does not lead to the conclusion. The statute (both the earlier and the current versions) says “damage” means “any impairment to the integrity or availability of data[etc.] ... that causes loss aggregating at least $5,000.” Multiple intrusions can cause a single impairment, and multiple corruptions of data can be described as a single “impairment” to the data. The statute does not say that an “impairment” has to result from a single intrusion, or has to be a single corrupted byte. A court construing a statute attributes a rational purpose to Congress. Getloaded’s construction would attribute obvious futility to Congress rather than rationality, because a hacker could evade the statute by setting up thousands of $4,999 (or millions of $4.99) intrusions. As the First Circuit pointed out in the analogous circumstance of physical impairment, so narrow a construction of the $5,000 impairment requirement would merely “reward sophisticated intruders.”46 The damage floor in the Computer Fraud and Abuse Act contains no “single act” requirement.

B. REGULATING BUSINESS RECORDS AND DATABASES
5. STATUTORY PROTECTIONS
(c) Video Privacy Protection Act

p. 664 – Insert new case before Notes & Questions:

DANIEL V. CANTELL
375 F.3d 377 (6th Cir. 2004)

CUDAHY, J. The plaintiff, Alden Joe Daniel, Jr. (Daniel) was charged with and eventually pleaded guilty to the sexual molestation of three underage girls. Allegedly, part of his modus operandi was showing pornographic movies to the underage girls. . . . Therefore, as part of the criminal investigation into his conduct, law enforcement officials sought and were able to obtain his video rental records. . . .

Daniel brings this suit against (1) various police officers, attorneys, and the parents of one of Daniel’s victims, as well as (2) the employees and owners of two video stores where Daniel rented pornographic videos. There is no dispute that the defendants making up this second category are proper parties under the Act. The only question which we must answer is whether the defendants not associated with the video stores are proper parties under the Act. We believe that based on the plain language of the Act, this first group of defendants are not proper parties. . . .

Section (b) provides that “[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).” 18 U.S.C. § 2710(b)(1) (emphasis added). Therefore, under the plain language of

46 EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir.2001).
the statute, only a “video tape service provider” (VTSP) can be liable. The term VTSP is defined by the statute to mean “any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio video materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.” Id. at § 2710(a)(4). Daniel does not allege that the defendants in question are engaged in the business of rental, sale or delivery of prerecorded video cassette tapes. Therefore, the defendants may only be VTSPs if personal information was disclosed to them under subparagraph (D) or (E) of subsection (b)(2).

Subparagraph (D) applies “if the disclosure is solely the names and addresses of consumers.” Id. at § 2710(b)(2)(D). Moreover, disclosure under subparagraph (D) must be “for the exclusive use of marketing goods and services directly to the consumer.” Id. at § 2710(b)(2)(D)(ii). For instance, if a video store provided the names and addresses of its patrons to a movie magazine publisher, the publisher would be considered a VTSP, but only with respect to the information contained in the disclosure. No disclosure in this case was made under subparagraph (D). The information provided was not limited to Daniel’s name and address. Instead, the disclosure was of Daniel’s history of renting pornographic videotapes and included the specific titles of those videos. Additionally, the disclosure was not for marketing purposes but for purposes of a criminal investigation. Therefore, subparagraph (D) is inapplicable in this case.

Daniel properly does not argue that the disclosure falls within subparagraph (E). … Subparagraph (E) applies only to disclosures made “incident to the ordinary course of business” of the VTSP. Id. at § 2710(b)(2)(E). The term “ordinary course of business” is “narrowly defined” in the statute to mean “only debt collection activities, order fulfillment, request processing, and the transfer of ownership.” Id. at § 2710(a)(2).

In sum, because Daniel has presented no evidence suggesting that a disclosure was made under subparagraph (D) or (E) in this case, the non-video store defendants are not VTSPs under the Act and therefore, are not proper parties to this litigation.

Daniel argues, however, that any person, not just a VTSP, can be liable under the Act based on Dirkes v. Borough of Runnemede, 936 F. Supp. 235 (D.N.J. 1996). Dirkes did reach this conclusion but only by misreading the Act. The court in Dirkes was focused on language in the Act stating that “[a]ny person aggrieved by any act of a person in violation of this section may bring a civil action in the United States district court.” 18 U.S.C. § 2710(c)(1) (emphasis added). Because the statute states that a suit can be based upon an act of “a person” rather than an act of “a VTSP,” Dirkes found that any person can be liable under the Act. Dirkes, however, ignored the rest of the sentence. A lawsuit under the Act must be based on an “act of a person in violation of this section ….” 18 U.S.C. § 2710(c)(1) (emphasis added). The statute makes it clear that only a VTSP can be in violation of section 2710(b). See § 2710(b)(1) (“A video tape service provider who knowingly discloses . . . personally identifiable information . . . shall be liable. . . .”). Moreover, if any person could be liable under the Act, there would be no need for the Act to define a VTSP in the first place. More tellingly, if any person could be liable under the Act, there is no reason that the definition of a VTSP would be limited to “any person . . . to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2).” Dirkes would have us ignore this limitation and find that any person
can be liable under the Act whether or not a disclosure was made to him under subparagraph (D) or (E). We avoid interpretations of a statute which would render portions of it superfluous.

The court in *Dirkes* found otherwise because the “clear intent of the Act,” as demonstrated by its legislative history, “is to prevent the disclosure of private information.” Where the plain language of a statute is clear, however, we do not consult the legislative history. . . . In any case, our interpretation of the statute—that only a VTSP can be liable under § 2710(b)—does not conflict with Congress’ purpose in adopting the Act. One can “prevent the disclosure of private information” simply by cutting off disclosure at its source, i.e., the VTSP. Just because Congress’ goal was to prevent the disclosure of private information, does not mean that Congress intended the implementation of every conceivable method of preventing disclosures. Printing all personal information in hieroglyphics instead of English would also help prevent the disclosure of such information. However, nothing in the legislative history suggests that Congress was encouraging hieroglyphics and, similarly, nothing suggests that Congress intended that anyone other than VTSPs would be liable under the Act. In sum, the Act is clear that only a VTSP can be liable under § 2710(b). Because the non-video store defendants do not fit within the definition of a VTSP, they are not proper parties.

p. 664– Insert new Note 2:

2. Rights of Action under the VPPA. The key question in *Dirkes*, *Video Software Dealers Ass’n*, and *Daniel* is whether the VPPA only regulates video tape service providers. The Sixth Circuit in *Daniel* answered this question affirmatively; the two other courts would apply the VPPA to additional parties, including law enforcement officers. Which interpretation of the statutory language do you find most convincing? Would policy reasons support a broader or narrower application of the statute? Should Congress enact a statutory fix to it to make it clear that the VPPA is to apply beyond video tape service providers?

B. REGULATING BUSINESS RECORDS AND DATABASES

5. STATUTORY PROTECTIONS

(f) Children’s Online Privacy Protection Act

p. 669- Insert new text after section (g):

*FTC Enforcement Actions.* The FTC has engaged in 12 enforcement actions pursuant to COPPA. These cases have resulted in settlements simultaneously with the filing of complaints. Heavy penalties have been assessed as part of some of the settlements. For example, in September 2006, the FTC announced a settlement with Xanga.com, which included a $1 million civil penalty. The complaint charges that Xanga.com, a social networking website, had actual knowledge of its collection of disclosure of children’s personal information. The Xanga website stated that children under 13 could not join its social network, but it allowed visitors to create Xanga accounts even if they provided a birth date indicating that they were younger than that age. Moreover, Xanga did not provide parents with access to and control over their
children’s information, and did not notify the parents of children who joined the site of its information practices. Finally, the FTC found that Xanga had created 1.7 million accounts for users who submitted age information that indicated they were younger than 13 years old.

In addition, the FTC has fined operators of websites in situations where they lacked actual knowledge that they were collecting information of someone who was under thirteen. Thus, the FTC found a violation of COPPA when a website was directed to children and provided a pull-down menu for the year of birth that did not include any of the last twelve years.47

6. FIRST AMENDMENT LIMITATIONS ON PRIVACY REGULATION

p. 686 – Add the following after note3:

4. The Value of Privacy. What is the value of protecting the privacy of consumer information maintained by telecommunications companies? Is it more important than the economic benefits that the telecommunications companies gain by using that information for marketing? How should policymakers go about answering such questions? Consider James Nehf:

The choice of utilitarian reasoning--often reduced to cost-benefit analysis ("CBA") in policy debates--fixes the outcome in favor of the side that can more easily quantify results. In privacy debates, this generally favors the side arguing for more data collection and sharing. Although CBA can mean different things in various contexts, the term here means a strategy for making choices in which quantifiable weights are given to competing alternatives.

We should openly acknowledge that non-economic values are legitimate in privacy debates, just as they have been recognized in other areas of fundamental importance. Decisions about the societal acceptance of disabled citizens, the codification of collective bargaining rights for workers, and the adoption of fair trial procedures for the accused did not depend entirely, or even primarily, on CBA outcomes. Difficulties in quantifying costs and benefits do not present insurmountable obstacles when policymakers address matters of basic human dignity. The protection of personal data should be viewed in a similar way, and CBA should play a smaller role in privacy debates.

A similar phenomenon is at work in the formulation of public policy. Policymakers are often asked to compare incomparable alternatives. By converting all values to money, the incomparability problem is lessened, but only if we accept the legitimacy of money as the covering value. In the privacy debate, the legitimacy of monetizing individual privacy preferences is highly suspect. Benefits are often personal, emotional, intangible, and not readily quantifiable. Preferences on privacy matters are generally muddled, incoherent, and ill-informed. If privacy preferences are real but not sufficiently coherent to form a sound basis for valuation, any attempt to place a monetary value on them loses meaning. The choice of CBA as the model for justifying decisions fixesthe end, because the chosen covering value will usually result in a decision favoring data proliferation over data protection.

People make choices between seemingly incomparable things all the time, and they can do so rationally. A person is not acting irrationally by preferring a perceived notable value over an incomparable nominal value, even if she cannot state a normative theory to explain why the decision is right. A similar phenomenon may be seen in the formulation of public policy. Notable values may be preferred over nominal ones in the enactment of laws and the implementation of policies even if policymakers cannot explain why one alternative is better than the other. Moreover, by observing a

number of such decisions over time, we may begin to see a pattern develop and covering values emerge that can serve as guides to later decisions that are closer to the margin.48

C. SPAM
3. SPAM AND SPEECH

p. 695 – Add the following before section 3:

A Critique of Anti-Spam Legislation. Consumers don’t always dislike marketing messages. As Eric Goldman reminds us, “consumers want marketing when it creates personal benefits for them, and marketing also can have spillover benefits that improve social welfare.” Goldman is worried that current legal regulation will block the kinds of filters that will improve the ability of consumers to manage information and receive information that will advance their interests. He points to anti-adware laws in Utah and Alaska as especially problematic; these statutes “prohibit client-side software from displaying pop-up ads triggered by the consumer’s use of a third party trademark or domain name—even if the consumer has fully consented to the software.” For Goldman, these statutes are flawed because they try to “ban or restrict matchmaking technologies.” The ideal filter would be a “mind-reading wonder” that “could costlessly—but accurately—read consumers’ minds, infer their expressed and latent preferences without the consumer bearing any disclosure costs, and act on the inferred preferences to screen out unwanted content and proactively seek out wanted content.” Goldman is confident that such filtering technology is not only possible, but “inevitable—perhaps imminently.”49 What kind of regulatory approach would encourage development and adoption of Goldman’s favored filters while also blocking existing SPAM technology? Will surrendering more privacy help better target marketing and thus clear out our inboxes of unwanted spam?

p. 700 – Insert the following before Section E: Information

Following California’s enactment of S.B. 1386, many other states enacted data breach notification laws. According to a tally from 2007, thirty-three states had enacted statutes that required governmental agencies and/or private companies to disclose security breaches involving personal information.50 Data breaches have also led to FTC enforcement actions and class action lawsuits under tort theories of negligence. We first will discuss these FTC actions and class action lawsuits, and then examine the data breach statutes.

FTC Enforcement Actions. The FTC has acted on nine occasions to penalize merchants that fail to take reasonable measures to protect customer data. In a typical data security complaint, the FTC argues that the firm’s data-handling practices constituted unfair acts or practices in violation of Section 5 of the Federal Trade Commission Act. In

settling its enforcement actions, the FTC has required both general and specific pledges of reasonable data security.

The most dramatic of these FTC enforcement actions involved ChoicePoint. In settling the FTC charges, ChoicePoint agreed to pay $10 million in civil penalties and $5 million into a consumer redress fund.\(^{51}\) It also promised changes to its business and improvements to its security practices. ChoicePoint agreed to “establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers.” In maintaining this “comprehensive information security program,” ChoicePoint promised to engage in risk assessments and to design and implement regular testing of the effectiveness of its security program’s key controls, systems, and procedures. It also agreed to obtain an initial and then biennial outside assessment of its data security safeguards from an independent third-party professional.

**Tort Law and Class Actions Suits.** In tort law, under a general negligence theory, litigants might also sue a company after a data security incident and seek to collect damages. Thus far, however, class action law suits following data breaches have been notably unsuccessful. Among other problems, claimants are facing trouble convincing courts that the data processing entities owe a duty to the individuals whose data are leaked, or that damages can be inferred from the simple fact of a data breach. For example, a South Carolina court declared in 2003 that “[t]he relationship, if any, between credit card issuers and potential victims of identity theft is far too attenuated to rise to the level of a duty between them.” *Huggins v. Citibank*, 585 S.E.2d 275 (S.C. 2003). Moreover, as the Seventh Circuit recently summarized the caselaw, “all of the cases rely on the same basic premise: Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy.” *Pisciotta v. Old Nat. Bancorp*, -- F.3d--, 2007 WL 2389770 (7th Cir. 2007).

**Data Breach Notification Statutes.** Within a few short years after the enactment of the California law, thirty-three states have enacted such statutes. These laws can be examined according to the following criteria: (1) the entities that the law covers; (2) the law’s trigger for notification; (3) any exceptions to the law’s notification requirement; (4) the party to whom disclosure is required under the law; (5) whether there is a substantive requirement for data security; and (6) the presence or absence of a private right of action.\(^{52}\)

Using these criteria, one sees that the California breach notification statute has had a strong influence on the other breach notification statutes. Twenty-three states follow the California approach and rely on the “acquisition” standard for breach notification. These states require notification whenever there is a reasonable likelihood that an unauthorized party has “acquired” person information. Only seven states have adopted a higher standard. These states consider whether there is a reasonable likelihood of “misuse” of the information, or “material risk” of harm to the person. The idea is that a breach letter should not be sent to the affected public unless there is a more significant

---


\(^{52}\) For a detailed chart examining these laws, state-by-state, see Schwartz-Janger, at 972-84.
likelihood of harm.

A mere three states provide a private right of action for individuals whose information has been breached. Finally, only eight of the state statutes create a substantive duty to take reasonable steps to safeguard data. Breach notification statutes in Arkansas, California, Nevada, North Carolina, Rhode Island, Texas, and Utah establish such a requirement. These seven state statutes provide open-ended, general standards, such as a requirement to provide “reasonable security procedures and practices appropriate to the nature of the information.” In California, such standards are supplemented by nonbinding, albeit more specific, recommendations from the Office of Privacy Protection.

As noted, most states rely on the same basic trigger for notification: a reasonable belief of “acquisition” of the leaked data. A minority of states require the likelihood of outside “misuse” of the information. The question is whether information may be acquired by an outside party, but not misused. More generally, breach notification letters may lose their effectiveness if consumers become dulled by frequent cautions about harms that never materialize. In this sense, Fred Cate writes “if the California law were adopted nationally, like the boy who cried wolf, the flood of notices would soon teach consumers to ignore them. When real danger threatened, who would listen?”

What kind of breach notification statute would be optimal? Schwarz and Janger do not wish to abandon the use of notification letters to the public-- in their view, within organizations, notification letters have the potential to (1) create a credible threat of negative costs or other punishments for the firm, (2) improve information flows within the firm, and (3) strengthen the position of the data security and privacy officers at the company. Moreover, breach notification letters can play an important role outside the breached organization. Mandated breach disclosure can trigger legislative and other regulatory activity. Schwarz and Janger argue:

As information about data security breaches and industry practices becomes public, the public, media, and legislators learn about the kinds of errors that lead to data breaches and the types of mistakes that companies make. This situation creates an opportunity for legislators to suggest new regulations and for governmental agencies to provide pressure as to the appropriate content of existing legal standards.

Schwartz and Janger propose that the critical need is for a “coordinated response architecture,” which would include a “coordinated response agent” (CRA) to help tailor notice content and supervise the decision whether to give notice. Notification to the consumer would follow upon a reasonable likelihood of “misuse” of notification-triggering information, and notification to the CRA would require the lower standard of a reasonable likelihood of “unauthorized access.” The CRA will help coordinate actions that companies take after a breach, tailor the content of the notification in light of the nature of the data breach, and help prepare comparative statistical information regarding data security events.

---

53 See, e.g., Fred H. Cate, Another Notice Isn’t an Answer, USA Today, Feb. 27, 2005, at 14A.
54 Schwartz-Janger, at 956.
Marcy Peek argues that the GLB Act has actually done more to facilitate information sharing than to protect privacy. Enabling greater information uses so long as customers have a right to opt-out has resulted in much more information sharing since “the opt-out right is meaningless in practice; the right to opt out of the trafficking of one’s personal information is explained in lengthy, legalistic privacy policies that most people throw away as just more junk mail.” More broadly, Peek argues, several laws purporting to protect privacy often “represent a façade of protection for consumers, keeping them complacent in the purported knowledge that someone is protecting their privacy interests.” In the end, Peek argues, “corporate power drives information privacy law.”

G. GOVERNMENT ACCESS TO FINANCIAL AND BUSINESS RECORDS

1. INFORMATION GATHERING WITHOUT SEARCH WARRANTS

(a) Administrative and Grand Jury Subpoenas

The government sought information for its use in ACLU v. Gonzales, No. 98-CV-5591, pending in the Eastern District of Pennsylvania. That case involved a challenge by the ACLU to the Children’s Online Protection Act (COPA). Google was not a party to that case, but the government subpoenaed from Google: (1) URL samples: “[a]ll URL’s that are available to be located to a query on your company’s search engine as of July 31, 2005” and (2) search queries: “[a]ll queries that have been entered on your company’s search engine between June 1, 2005 and July 31, 2005 inclusive.” Subsequently, the government narrowed its URL sample demand to 50,000 URLs and it narrowed its search query demand to all queries during a 1-week period rather than the two-month period mentioned above. Google still raised a challenge, and the government again narrowed its search query request for only 5,000 entries from Google’s query log. It continued to seek a sample of 50,000 URLs from Google’s search index. Under Federal Rule of Civil Procedure 26, a subpoena sought must be “reasonably calculated to lead to admissible evidence.” It may be quashed if the “burden or expense of the proposed discovery outweighs its likely benefit.”

WARE, J. . . . As narrowed by negotiations with Google and through the course of this Miscellaneous Action, the Government now seeks a sample of 50,000 URLs from Google’s search index. In determining whether the information sought is reasonably calculated to lead to admissible evidence, the party seeking the information must first
provide the Court with its plans for the requested information. The Government’s disclosure of its plans for the sample of URLs is incomplete. The actual methodology disclosed in the Government’s papers as to the search index sample is, in its entirety, as follows: “A human being will browse a random sample of 5,000-10,000 URLs from Google’s index and categorize those sites by content” and from this information, the Government intends to “estimate...the aggregate properties of the websites that search engines have indexed.” The Government’s disclosure only describes its methodology for a study to categorize the URLs in Google’s search index, and does not disclose a study regarding the effectiveness of filtering software. Absent any explanation of how the “aggregate properties” of material on the Internet is germane to the underlying litigation, the Government’s disclosure as to its planned categorization study is not particularly helpful in determining whether the sample of Google’s search index sought is reasonably calculated to lead to admissible evidence in the underlying litigation.

Based on the Government’s statement that this information is to act as a “test set for the study” and a general statement that the purpose of the study is to “evaluate the effectiveness of content filtering software,” the Court is able to envision a study whereby a sample of 50,000 URLs from the Google search index may be reasonably calculated to lead to admissible evidence on measuring the effectiveness of filtering software. In such a study, the Court imagines, the URLs would be categorized, run through the filtering software, and the effectiveness of the filtering software ascertained as to the various categories of URLs. The Government does not even provide this rudimentary level of general detail as to what it intends to do with the sample of URLs to evaluate the effectiveness of filtering software, and at the hearing neither confirmed nor denied the Court’s speculations about the study. In fact, the Government seems to indicate that such a study is not what it has in mind: “[t]he government seeks this information only to perform a study, in the aggregate, of trends on the Internet” (emphasis added), with no explanation of how an aggregate study of Internet trends would be reasonably calculated to lead to admissible evidence in the underlying suit where the efficacy of filtering software is at issue. . . .

Given the broad definition of relevance in Rule 26, and the current narrow scope of the subpoena, despite the vagueness with which the Government has disclosed its study, the Court gives the Government the benefit of the doubt. The Court finds that the 50,000 URLs randomly selected from Google’s database for use in a scientific study of the effectiveness of filters is relevant to the issues in the case of ACLU v. Gonzales. 56

In its original subpoena the Government sought a listing of the text of all search queries entered by Google users over a two month period. As defined in the Government’s subpoena, “queries” include only the text of the search string entered by a user, and not “any additional information that may be associated with such a text string that would identify the person who entered the text string into the search engine, or the computer from which the text string was entered.” The Government has narrowed its request so that it now seeks only a sample of 5,000 such queries from Google’s query log. The Government discloses its plans for the query log information as follows: “A random

56 To the extent that the Government is gathering this information for some other purpose than to run the sample of Google’s search index through various filters to determine the efficacy of those filters, the Court would take a different view of the relevance of the information. For example, the Court would not find the information relevant if it is being sought just to characterize the nature of the URL’s in Google’s database.
sample of approximately 1,000 Google queries from a one-week period will be run through the Google search engine. A human being will browse the top URLs returned by each search and categorize the sites by content.” . . .

Google also argues that it will be unduly burdened by loss of user trust if forced to produce its users’ queries to the Government. Google claims that its success is attributed in large part to the volume of its users and these users may be attracted to its search engine because of the privacy and anonymity of the service. According to Google, even a perception that Google is acquiescing to the Government’s demands to release its query log would harm Google’s business by deterring some searches by some users.

Google’s own privacy statement indicates that Google users could not reasonably expect Google to guard the query log from disclosure to the Government. . . . Google’s privacy policy does not represent to users that it keeps confidential any information other than “personal information.” Neither Google’s URLs nor the text of search strings with “personal information” redacted, are reasonably “personal information” under Google’s stated privacy policy. Google’s privacy policy indicates that it has not suggested to its users that non-”personal information” such as that sought by the Government is kept confidential.

However, even if an expectation by Google users that Google would prevent disclosure to the Government of its users’ search queries is not entirely reasonable, the statistic cited by Dr. Stark that over a quarter of all Internet searches are for pornography indicates that at least some of Google’s users expect some sort of privacy in their searches. The expectation of privacy by some Google users may not be reasonable, but may nonetheless have an appreciable impact on the way in which Google is perceived, and consequently the frequency with which users use Google. Such an expectation does not rise to the level of an absolute privilege, but does indicate that there is a potential burden as to Google’s loss of goodwill if Google is forced to disclose search queries to the Government.

Rule 45(c)(3)(B) provides additional protections where a subpoena seeks trade secret or confidential commercial information from a nonparty. . . . Because Google still continues to claim information about its entire search index and entire query log as confidential, the Court will presume that the requested information, as a small sample of proprietary information, may be somewhat commercially sensitive, albeit not independently commercially sensitive. Successive disclosures, whether in this lawsuit or pursuant to subsequent civil subpoenas, in the aggregate could yield confidential commercial information about Google’s search index or query log. . . .

What the Government has not demonstrated, however, is a substantial need for both the information contained in the sample of URLs and sample of search query text. Furthermore, even if the information requested is not a trade secret, a district court may in its discretion limit discovery on a finding that “the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive.” Rule 26(b)(2)(i).

Faced with duplicative discovery, and with the Government not expressing a preference as to which source of the test set of URLs it prefers, this Court exercises its discretion pursuant to Rule 26(b)(2) and determines that the marginal burden of loss of trust by Google’s users based on Google’s disclosure of its users’ search queries to the Government outweighs the duplicative disclosure’s likely benefit to the Government’s
study. Accordingly, the Court grants the Government’s motion to compel only as to the sample of 50,000 URLs from Google’s search index.

The Court raises, sua sponte, its concerns about the privacy of Google’s users apart from Google’s business goodwill argument.

Although the Government has only requested the text strings entered (Subpoena at 4), basic identifiable information may be found in the text strings when users search for personal information such as their social security numbers or credit card numbers through Google in order to determine whether such information is available on the Internet. The Court is also aware of so-called “vanity searches,” where a user queries his or her own name perhaps with other information. . . . This concern, combined with the prevalence of Internet searches for sexually explicit material—generally not information that anyone wishes to reveal publicly—gives this Court pause as to whether the search queries themselves may constitute potentially sensitive information.

The Court also recognizes that there may be a difference between a private litigant receiving potentially sensitive information and having this information be produced to the Government pursuant to civil subpoena. . . . Even though counsel for the Government assured the Court that the information received will only be used for the present litigation, it is conceivable that the Government may have an obligation to pursue information received for unrelated litigation purposes under certain circumstances regardless of the restrictiveness of a protective order. The Court expressed this concern at oral argument as to queries such as “bomb placement white house,” but queries such as “communist berkeley parade route protest war” may also raise similar concerns. In the end, the Court need not express an opinion on this issue because the Government’s motion is granted only as to the sample of URLs and not as to the log of search queries.

The Court also refrains from expressing an opinion on the applicability of the Electronic Communications Privacy Act. . . . The Court only notes that the ECPA does not bar the Government’s request for sample of 50,000 URLs from Google’s index through civil subpoena.

NOTES & QUESTIONS

1. URL Samples vs. Search Queries. The sought-after subpoena in Gonzales v. Google concerned information about both URL samples and search queries. What decision did the district court reach for each type of data? Are there different privacy implications for governmental access to the two kinds of information?

2. Can People Be Identified from Anonymous Search Data? An incident involving AOL proved that individuals can be identified based on their search queries. In August 2006, AOL revealed that it had released to researchers about 20 million search queries made by over 650,000 users of its search engine. Although AOL had substituted numerical IDs for the subscribers’ actual user names, the personal identity of the user could be found based on the search queries. The New Times demonstrated as much by tracking down AOL user No. 4417749; it linked this person’s data trail to a 62-year old widow who lived in Lilburn, Georgia and admitted to the reporter, “Those are my searches.”

57 Michael Barbaro & Tom Zeller, Jr., A Face is Exposed for AOL Searcher No. 4417749, N.Y. Times, Aug. 9, 2006.
G. GOVERNMENT ACCESS TO FINANCIAL AND BUSINESS RECORDS
1. INFORMATION GATHERING WITHOUT SEARCH WARRANTS
   (c) The USA-Patriot Act § 215 and National Security Letters

p. 735- Insert new noted after note 3:

4. OIG Report on NSLs. In its USA PATRIOT Reauthorization Act, Congress required a detailed examination by the DOJ’s Inspector General “of the effectiveness and use, including any improper or illegal use” of NSLs. 58 This kind of audit proved its value in March 2006 when the Inspector General issued its review of the FBI’s use of of NSLs. First, the Inspector General found a dramatic underreporting of NSLs. Indeed, the total number of NSL requests between 2003 and 2005 totaled at least 143,074. 59 Of these NSLs requests, as the IG found, “[t]he overwhelming majority … sought telephone toll billing records information, subscriber information (telephone or e-mail) or electronic communication transaction records under the ECPA NSL statute.” 60

The Inspector General also carried out a limited audit of investigative case files, and found that 22 percent of them contained at least one violation of investigative guidelines or procedures that was not reported to any of the relevant internal authorities at the FBI. Finally, the Inspector General also found over 700 instances in which the FBI obtained telephone records and subscriber information from telephone companies based on the use of a so-called “exigent letter” authority. This authority, absent from the statute, was invented by the FBI’s Counterterrorism Division. Having devised this new power, the FBI did not set limits on its use, or track how it was employed. Witnesses told the Inspector General that many of these letters “were not issued in exigent circumstances, and the FBI was unable to determine which letters were sent in emergency circumstances due to inadequate recordkeeping.” 61

5. Litigation about NSLs. In Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), a District Court in N.Y. invalidated 18 U.S.C. § 2709 (Doe I). It found that § 2709 violated the Fourth Amendment because, at least as applied, it barred or at least substantially deterred a judicial challenge to a NSL request. It did so by prohibiting a NSL recipient from revealing the existence of a NSL inquiry. The court also found that the “all inclusive sweep” of § 2709 violated the First Amendment as a prior-restraint and content-based restriction on sweep that was subject to strict scrutiny review. Shortly thereafter, a District Court in Connecticut invalidated 18 U.S. § 2709(c), which prevented a recipient of a NSL to disclose information about the government's action. Doe v. Gonzales, 386 F. Supp. 2d 66, 82 (D. Conn. 2005) (Doe II).

While appeals in Doe I and Doe II were pending, Congress enacted the USA Patriot Reauthorization Act of 2005, which made several changes to § 2709 and added

---

58 USA Patriot Reauthorization Act, at § 119(a).
60 Id.
61 Id. at xxxviii. Indeed, “in most instances, there was no documentation associating the requests with pending national security investigations.” Id. at xxxiv.
several provisions concerning judicial review of NSLs, which were codified at 18 U.S.C. § 3511. Following enactment of these provisions, plaintiffs challenged the amended nondisclosure provisions of § 2709(c) and § 3511. The same District Court that issued the Doe I opinion then found § 2709(c) and § 3511(b) to be facially unconstitutional. Doe v. Gonzales, 2007 U.S. Dist. LEXIS 65879 (S.D.N.Y) (Doe III).

The newly enacted § 3511 provided for judicial review of NSLs. As a result, the Doe III plaintiffs did not challenge it on Fourth Amendment grounds as in Doe I. Instead, they argued, and the court agreed, that the nondisclosure provisions of § 2709(c) remained an unconstitutional prior restraint and content-based restriction on speech. The court also concluded that § 3511(b) was unconstitutional under the First Amendment and the doctrine of separation of powers. Among its conclusions, the court noted that Congress in amending § 2709(c) allowed the FBI to certify on a case-by-case basis whether nondisclosure was necessary. Yet, this narrowing of the statute to reduce the possibility of unnecessary limitation of speech also mean that the FBI could conceivably engage in viewpoint discrimination. As a consequence, the amended statute was a content-based restriction as well as a prior restraint on speech and, therefore, subject to strict scrutiny.

H. PRIVACY POLICIES: PRIVATE vs. PUBLIC ENFORCEMENT
2. PRIVATE ENFORCEMENT: CONTRACT REMEDIES

p. 750 – Add the following at the end of note 1:

Similarly, in In re Jet Blue Airways Corp. Privacy Litigation, 379 F. Supp. 2d 299 (E.D.N.Y. 2005), a group of plaintiffs sued Jet Blue Airlines for breach of contract for sharing passenger records with the government. Jet Blue moved to dismiss. The court held:

An action for breach of contract under New York law requires proof of four elements: (1) the existence of a contract, (2) performance of the contract by one party, (3) breach by the other party, and (4) damages.

With regard to the existence of a contract, plaintiffs contend that JetBlue undertook a “self-imposed contractual obligation by and between [itself] and the consumers with whom it transacted business” by publishing privacy policies on its website or otherwise disclosing such policies to its consumers. Plaintiffs maintain that “these self-imposed public assurances ... created an obligation under the contract-of-carriage and a duty on the part of JetBlue and the persons with whom it did business not to act in derogation of JetBlue’s privacy policy. . . .” JetBlue counters that its “stand-alone privacy statement”--which “could only be accessed and viewed by clicking on a separate stand-alone link” on the bottom of JetBlue’s website--is not a term in the contract of carriage. It further notes in this connection that “the entire transaction of purchasing transportation can be done on JetBlue’s website (or by phone or in person) without ever viewing, reading, or relying on JetBlue’s website privacy statement. . . .” Although plaintiffs do allege that the privacy policy constituted a term in the contract of carriage, they argue alternatively that a stand-alone contract was formed at the moment they made flight reservations in reliance on express promises contained in JetBlue’s privacy policy. JetBlue posits no persuasive argument why this alternative formulation does not form the basis of a contract.

JetBlue further argues that failure to allege that plaintiffs read the privacy policy defeats any claim of reliance. Although plaintiffs do not explicitly allege that the class members actually read or saw the privacy policy, they do allege that they and other class members relied on the
representations and assurances contained in the privacy policy when choosing to purchase air transportation from JetBlue. Reliance presupposes familiarity with the policy. It may well be that some members of the class did not read the privacy policy and thus could not have relied on it, but the issue of who actually read and relied on the policy would be addressed more properly at the class certification stage. For purposes of this motion, the Court considers an allegation of reliance to encompass an allegation that some putative members of the class read or viewed the privacy policy. The Court recognizes that contrary authority exists on this point, but considers the holding in that case to rest on an overly narrow reading of the pleadings. See In re Northwest (“[A]bsent an allegation that Plaintiffs actually read the privacy policy, not merely the general allegation that Plaintiffs ‘relied on’ the policy, Plaintiffs have failed to allege an essential element of a contract claim: that the alleged ‘offer’ was accepted by Plaintiffs.”). Accordingly, failure to specifically allege that all plaintiffs and class members read the policy does not defeat the existence of a contract for purposes of this motion to dismiss.

JetBlue also argues that plaintiffs have failed to meet their pleading requirement with respect to damages, citing an absence of any facts in the Amended Complaint to support this element of the claim. Plaintiffs’ sole allegation on the element of contract damages consists of the statement that JetBlue’s breach of the company privacy policy injured plaintiffs and members of the class and that JetBlue is therefore liable for “actual damages in an amount to be determined at trial.” . . . . At oral argument, when pressed to identify the “injuries” or damages referred to in the Amended Complaint, counsel for plaintiffs stated that the “contract damage could be the loss of privacy,” acknowledging that loss of privacy “may” be a contract damage. The support for this proposition was counsel’s proffer that he had never seen a case that indicates that loss of privacy cannot as a matter of law be a contract damage. In response to the Court’s inquiry as to whether a further specification of damages could be set forth in a second amended complaint, counsel suggested only that perhaps it could be alleged or argued that plaintiffs were deprived of the “economic value” of their information. Despite being offered the opportunity to expand their claim for damages, plaintiffs failed to proffer any other element or form of damages that they would seek if given the opportunity to amend the complaint. . . .

It is apparent based on the briefing and oral argument held in this case that the sparseness of the damages allegations is a direct result of plaintiffs’ inability to plead or prove any actual contract damages. As plaintiffs’ counsel concedes, the only damage that can be read into the present complaint is a loss of privacy. At least one recent case has specifically held that this is not a damage available in a breach of contract action. See Trikas v. Universal Card Services Corp., 351 F.Supp.2d 37, 46 (E.D.N.Y.2005). This holding naturally follows from the well-settled principle that “recovery in contract, unlike recovery in tort, allows only for economic losses flowing directly from the breach.”

Plaintiffs allege that in a second amended complaint, they could assert as a contract damage the loss of the economic value of their information, but while that claim sounds in economic loss, the argument ignores the nature of the contract asserted. . . . [T]he purpose of contract damages is to put a plaintiff in the same economic position he or she would have occupied had the contract been fully performed.” Plaintiffs may well have expected that in return for providing their personal information to JetBlue and paying the purchase price, they would obtain a ticket for air travel and the promise that their personal information would be safeguarded consistent with the terms of the privacy policy. They had no reason to expect that they would be compensated for the “value” of their personal information. In addition, there is absolutely no support for the proposition that the personal information of an individual JetBlue passenger had any value for which that passenger could have expected to be compensated. . . . . There is likewise no support for the proposition that an individual passenger’s personal information has or had any compensable value in the economy at large.

Accordingly, plaintiffs having claimed no other form of damages apart from those discussed herein and having sought no other form of relief in connection with the breach of contract claim, JetBlue’s motion to dismiss the claim is granted.

How does the JetBlue court’s analysis differ from that in Northwest Airlines? How is it similar?
4. Enforcing Privacy Policies as Contracts Against Consumers. Suppose privacy policies were enforceable as contracts. Would this be beneficial to consumers? It might not be, Allyson Haynes argues:

[T]here is a distinct possibility that as website operators grow savvier with respect to the law, they will respond to the lack of substantive privacy protection (and lack of consumer awareness) by including in privacy policies terms that are not favorable to consumers.

On the flip side of consumers seeking to enforce privacy policies as contracts, companies might also desire to hold customers to be contractually bound to the companies’ privacy policies. Would a privacy policy be enforceable as a contract against the customer? Haynes contends:

[P]articularly in cases where consumers are deemed to have assented to privacy policies by virtue of their presence on the site or by giving information without affirmatively clicking acceptance, the consumer has a good argument that he or she did not assent to the privacy policy, preventing the formation of a binding contract, and preventing the website from enforcing any of its terms against the consumer.62

---

A. PRIVACY AT HOME

p. 778 – Add the following at the end of Part A:

GEORGIA V. RANDOLPH

SOUTER, J. . . . The Fourth Amendment recognizes a valid warrantless entry and search of premises when police obtain the voluntary consent of an occupant who shares, or is reasonably believed to share, authority over the area in common with a co-occupant who later objects to the use of evidence so obtained. Illinois v. Rodriguez, 497 U.S. 177, 110 S.Ct. 2793, 111 L.Ed.2d 148 (1990); United States v. Matlock, 415 U.S. 164, 94 S.Ct. 988, 39 L.Ed.2d 242 (1974). The question here is whether such an evidentiary seizure is likewise lawful with the permission of one occupant when the other, who later seeks to suppress the evidence, is present at the scene and expressly refuses to consent. We hold that, in the circumstances here at issue, a physically present co-occupant’s stated refusal to permit entry prevails, rendering the warrantless search unreasonable and invalid as to him.

Respondent Scott Randolph and his wife, Janet, separated in late May 2001, when she left the marital residence in Americus, Georgia, and went to stay with her parents in
Canada, taking their son and some belongings. In July, she returned to the Americus house with the child, though the record does not reveal whether her object was reconciliation or retrieval of remaining possessions.

On the morning of July 6, she complained to the police that after a domestic dispute her husband took their son away, and when officers reached the house she told them that her husband was a cocaine user whose habit had caused financial troubles. She mentioned the marital problems and said that she and their son had only recently returned after a stay of several weeks with her parents. Shortly after the police arrived, Scott Randolph returned and explained that he had removed the child to a neighbor’s house out of concern that his wife might take the boy out of the country again; he denied cocaine use, and countered that it was in fact his wife who abused drugs and alcohol.

One of the officers, Sergeant Murray, went with Janet Randolph to reclaim the child, and when they returned she not only renewed her complaints about her husband’s drug use, but also volunteered that there were ‘‘items of drug evidence’’ in the house. Brief for Petitioner 3. Sergeant Murray asked Scott Randolph for permission to search the house, which he unequivocally refused.

The sergeant turned to Janet Randolph for consent to search, which she readily gave. She led the officer upstairs to a bedroom that she identified as Scott’s, where the sergeant noticed a section of a drinking straw with a powdery residue he suspected was cocaine. He then left the house to get an evidence bag from his car and to call the district attorney’s office, which instructed him to stop the search and apply for a warrant. When Sergeant Murray returned to the house, Janet Randolph withdrew her consent. The police took the straw to the police station, along with the Randolphs. After getting a search warrant, they returned to the house and seized further evidence of drug use, on the basis of which Scott Randolph was indicted for possession of cocaine.

He moved to suppress the evidence, as products of a warrantless search of his house unauthorized by his wife’s consent over his express refusal. . . .

To the Fourth Amendment rule ordinarily prohibiting the warrantless entry of a person’s house as unreasonable per se, one “jealously and carefully drawn” exception recognizes the validity of searches with the voluntary consent of an individual possessing authority. That person might be the householder against whom evidence is sought or a fellow occupant who shares common authority over property, when the suspect is absent, and the exception for consent extends even to entries and searches with the permission of a co-occupant whom the police reasonably, but erroneously, believe to possess shared authority as an occupant. None of our co-occupant consent-to-search cases, however, has presented the further fact of a second occupant physically present and refusing permission to search, and later moving to suppress evidence so obtained. The significance of such a refusal turns on the underpinnings of the co-occupant consent rule, as recognized since Matlock.

The defendant in that case was arrested in the yard of a house where he lived with a Mrs. Graff and several of her relatives, and was detained in a squad car parked nearby. When the police went to the door, Mrs. Graff admitted them and consented to a search of the house. . . .

The constant element in assessing Fourth Amendment reasonableness in the consent cases, then, is the great significance given to widely shared social expectations, which are naturally enough influenced by the law of property, but not controlled by its
rules. Matlock accordingly not only holds that a solitary co-inhabitant may sometimes consent to a search of shared premises, but stands for the proposition that the reasonableness of such a search is in significant part a function of commonly held understanding about the authority that co-inhabitants may exercise in ways that affect each other’s interests.

Matlock’s example of common understanding is readily apparent. When someone comes to the door of a domestic dwelling with a baby at her hip, as Mrs. Graff did, she shows that she belongs there, and that fact standing alone is enough to tell a law enforcement officer or any other visitor that if she occupies the place along with others, she probably lives there subject to the assumption tenants usually make about their common authority when they share quarters. They understand that any one of them may admit visitors, with the consequence that a guest obnoxious to one may nevertheless be admitted in his absence by another. As Matlock put it, shared tenancy is understood to include an “assumption of risk,” on which police officers are entitled to rely, and although some group living together might make an exceptional arrangement that no one could admit a guest without the agreement of all, the chance of such an eccentric scheme is too remote to expect visitors to investigate a particular household’s rules before accepting an invitation to come in. So, Matlock relied on what was usual and placed no burden on the police to eliminate the possibility of atypical arrangements, in the absence of reason to doubt that the regular scheme was in place. . . .

Although we have not dealt directly with the reasonableness of police entry in reliance on consent by one occupant subject to immediate challenge by another, we took a step toward the issue in an earlier case dealing with the Fourth Amendment rights of a social guest arrested at premises the police entered without a warrant or the benefit of any exception to the warrant requirement. Minnesota v. Olson, 495 U.S. 91 (1990), held that overnight houseguests have a legitimate expectation of privacy in their temporary quarters because “it is unlikely that [the host] will admit someone who wants to see or meet with the guest over the objection of the guest.” If that customary expectation of courtesy or deference is a foundation of Fourth Amendment rights of a houseguest, it presumably should follow that an inhabitant of shared premises may claim at least as much, and it turns out that the co-inhabitant naturally has an even stronger claim.

To begin with, it is fair to say that a caller standing at the door of shared premises would have no confidence that one occupant’s invitation was a sufficiently good reason to enter when a fellow tenant stood there saying, “stay out.” Without some very good reason, no sensible person would go inside under those conditions. Fear for the safety of the occupant issuing the invitation, or of someone else inside, would be thought to justify entry, but the justification then would be the personal risk, the threats to life or limb, not the disputed invitation.

The visitor’s reticence without some such good reason would show not timidity but a realization that when people living together disagree over the use of their common quarters, a resolution must come through voluntary accommodation, not by appeals to authority. Unless the people living together fall within some recognized hierarchy, like a household of parent and child or barracks housing military personnel of different grades, there is no societal understanding of superior and inferior, a fact reflected in a standard formulation of domestic property law, that “[e]ach cotenant ... has the right to use and enjoy the entire property as if he or she were the sole owner, limited only by the same
right in the other cotenants.” . . . In sum, there is no common understanding that one co-tenant generally has a right or authority to prevail over the express wishes of another, whether the issue is the color of the curtains or invitations to outsiders.

Since the co-tenant wishing to open the door to a third party has no recognized authority in law or social practice to prevail over a present and objecting co-tenant, his disputed invitation, without more, gives a police officer no better claim to reasonableness in entering than the officer would have in the absence of any consent at all. Accordingly, in the balancing of competing individual and governmental interests entailed by the bar to unreasonable searches, the cooperative occupant’s invitation adds nothing to the government’s side to counter the force of an objecting individual’s claim to security against the government’s intrusion into his dwelling place. Since we hold to the “centuries-old principle of respect for the privacy of the home,” Wilson v. Layne, 526 U.S. 603 (1999), “it is beyond dispute that the home is entitled to special protection as the center of the private lives of our people,” Minnesota v. Carter, 525 U.S. 83 (1998) (Kenndedy, J., concurring). . . .

Disputed permission is thus no match for this central value of the Fourth Amendment, and the State’s other countervailing claims do not add up to outweigh it. . . .

ROBERTS & SCALIA, J.J. DISSENTING. The Fourth Amendment protects privacy. If an individual shares information, papers, or places with another, he assumes the risk that the other person will in turn share access to that information or those papers or places with the government. And just as an individual who has shared illegal plans or incriminating documents with another cannot interpose an objection when that other person turns the information over to the government, just because the individual happens to be present at the time, so too someone who shares a place with another cannot interpose an objection when that person decides to grant access to the police, simply because the objecting individual happens to be present.

A warrantless search is reasonable if police obtain the voluntary consent of a person authorized to give it. Co-occupants have “assumed the risk that one of their number might permit [a] common area to be searched.” United States v. Matlock, 415 U.S. 164 (1974). Just as Mrs. Randolph could walk upstairs, come down, and turn her husband’s cocaine straw over to the police, she can consent to police entry and search of what is, after all, her home, too . . . .

[T]he majority is confident in assuming--confident enough to incorporate its assumption into the Constitution--that an invited social guest who arrives at the door of a shared residence, and is greeted by a disagreeable co-occupant shouting “’stay out,’” “would simply go away. The Court observes that “no sensible person would go inside under those conditions,” and concludes from this that the inviting co-occupant has no “authority” to insist on getting her way over the wishes of her co-occupant, But it seems equally accurate to say--based on the majority’s conclusion that one does not have a right to prevail over the express wishes of his co-occupant--that the objector has no “authority” to insist on getting his way over his co-occupant’s wish that her guest be admitted.

The fact is that a wide variety of differing social situations can readily be imagined, giving rise to quite different social expectations. A relative or good friend of one of two feuding roommates might well enter the apartment over the objection of the other roommate. The reason the invitee appeared at the door also affects expectations: A
guest who came to celebrate an occupant’s birthday, or one who had traveled some distance for a particular reason, might not readily turn away simply because of a roommate’s objection. The nature of the place itself is also pertinent: Invitees may react one way if the feuding roommates share one room, differently if there are common areas from which the objecting roommate could readily be expected to absent himself. Altering the numbers might well change the social expectations: Invitees might enter if two of three co-occupants encourage them to do so, over one dissenter.

In United States v. White, we held that one party to a conversation can consent to government eavesdropping, and statements made by the other party will be admissible at trial. This rule is based on privacy: “Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police .... [I]f he has no doubts, or allays them, or risks what doubt he has, the risk is his.”

As the Court explained in United States v. Jacobsen:

It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information: ‘This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in a third party will not be betrayed.’

The same analysis applies to the question whether our privacy can be compromised by those with whom we share common living space. If a person keeps contraband in common areas of his home, he runs the risk that his co-occupants will deliver the contraband to the police.

Even in our most private relationships, our observable actions and possessions are private at the discretion of those around us. A husband can request that his wife not tell a jury about contraband that she observed in their home or illegal activity to which she bore witness, but it is she who decides whether to invoke the testimonial marital privilege.

There is no basis for evaluating physical searches of shared space in a manner different from how we evaluated the privacy interests in the foregoing cases.

The common thread in our decisions upholding searches conducted pursuant to third-party consent is an understanding that a person “assume[s] the risk” that those who have access to and control over his shared property might consent to a search. Matlock, 415 U.S., at 171. In Matlock, we explained that this assumption of risk is derived from a third party’s “joint access or control for most purposes” of shared property. And we concluded that shared use of property makes it “reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right.”

In this sense, the risk assumed by a joint occupant is comparable to the risk assumed by one who reveals private information to another. If a person has incriminating information, he can keep it private in the face of a request from police to share it, because he has that right under the Fifth Amendment. If a person occupies a house with incriminating information in it, he can keep that information private in the face of a request from police to search the house, because he has that right under the Fourth Amendment. But if he shares the information—or the house—with another, that other can grant access to the police in each instance.
Just as the source of the majority’s rule is not privacy, so too the interest it protects cannot reasonably be described as such. That interest is not protected if a co-owner happens to be absent when the police arrive, in the backyard gardening, asleep in the next room, or listening to music through earphones so that only his co-occupant hears the knock on the door. That the rule is so random in its application confirms that it bears no real relation to the privacy protected by the Fourth Amendment. What the majority’s rule protects is not so much privacy as the good luck of a co-owner who just happens to be present at the door when the police arrive.

Rather than draw such random and happenstance lines—and pretend that the Constitution decreed them—the more reasonable approach is to adopt a rule acknowledging that shared living space entails a limited yielding of privacy to others, and that the law historically permits those to whom we have yielded our privacy to in turn cooperate with the government. Such a rule flows more naturally from our cases concerning Fourth Amendment reasonableness and is logically grounded in the concept of privacy underlying that Amendment.

NOTES & QUESTIONS

1. Presence Versus Absence. In United States v. Matlock, 415 U.S. 164 (1974), the Supreme Court held that the “consent of one who possesses common authority over premises or effects is valid as against the absent, nonconsenting person with whom that authority is shared.” In Illinois v. Rodriguez, 497 U.S. 177 (1990), the Court held that even if the police wrongly believe that the person consenting to the search has authority over the property, the search is valid so long as the police error was reasonable and in good faith. The difference in Randolph is that the defendant was home at the time and did not consent. Had he been absent, the police would have been able to search under the Fourth Amendment. Does this distinction make sense?

2. Assumption of Risk. Is Chief Justice Roberts correct that the assumption of risk doctrine should govern this case? Suppose Scott Randolph’s wife went to the cops and gave information about Scott’s criminal activity. There would be no Fourth Amendment problem here. So why can’t she let the police into her house to show the police the same information?

p. 794-96 - Insert new material to replace existing text:

B. PRIVACY AT SCHOOL

3. SCHOOL RECORDS

THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

The Family Educational Rights and Privacy Act (FERPA) of 1974, Pub. L. No. 93-380, 20 U.S.C. § 1232g, commonly known as the “Buckley Amendment,” generally prohibits schools from releasing student “education records” without the authorization of the student and/or parent. Schools may release such “directory” information as names, addresses, dates of attendance, degrees earned, and activities unless the student and/or
parent expressly indicates in writing that he or she wants it to remain confidential.

FERPA covers only records and information from records, not information per se. Thus, school authorities’ personal knowledge and observations that are not part of a record are not covered. See *Frasca v. Andrews*, 463 F. Supp. 1043, 1050 (E.D.N.Y. 1979) (“Congress could not have constitutionally prohibited comment on, or discussion of, facts about a student which were learned independently of his school records.”) As a result, FERPA does not apply to “personal knowledge derived from direct, personal experience with a student.” For example, an employee of an educational institution, such as a faculty or staff member, can share information with others if she “personally observes a student engaging in erratic and threatening behavior.”

**Education Records.** “Education records” are “those records, files, documents, and other materials which contain information directly related to a student; and are maintained by an educational agency or institution.” 20 U.S.C. § 1232g(a)(4)(A). “Law enforcement unit records” and certain medical treatment records maintained by school officials do not constitute education records., § 1232g(a)(4)(B), but virtually all other institutional records that are personally identifiable to one or more students are covered.

**Notice.** Schools must inform students and parents of their rights under FERPA. See 34 C.F.R. § 99.7.

**Access and Ability to Correct Errors.** Schools generally must provide students and/or parents with access to their education records — a chance to review their records upon request. § 1232g(a)(1)(A). Schools must provide the student with an opportunity for a hearing “to challenge the content of such student’s education records, in order to insure that the records are not inaccurate, misleading, or otherwise in violation of the privacy or other rights of students, and to provide an opportunity for the correction or deletion of any inaccurate, misleading, or otherwise inappropriate data contained therein. . . .” § 1232g(a)(2).

**Limits on Disclosure.** Pursuant to § 1232g(b), schools cannot disclose a student’s education records without written consent. Certain disclosures are exempted from this rule. For example, the school can disclose records to “school officials” with a “legitimate educational interest,” to appropriate persons in order to protect health or safety of the student or others, as well as to a number of other entities and officials. § 1232g(b)(1). If the student does not opt out, a school may release to the public the student’s name, address, telephone numbers, birth date, major, activities and sports, dates of attendance, degrees and awards received, and certain other such “directory” information. § 1232g(b)(5).

**Enforcement.** FERPA authorizes the Secretary of Education to end all federal funding if a school fails to comply with the statute. § 1232g(f). The Department of Education’s Family Policy Compliance Office oversees the enforcement of FERPA. See 34 C.F.R. § 99.60(b). Before the Compliance Office takes action, an individual must file

---

63 Nancy E. Tribbensee & Steven J. McDonald, *FERPA and Campus Safety*, 5 NACU Notes (No. 4, Aug. 6, 2007).

64 Id.
a complaint against a school. The Compliance Office then investigates and if the school is found in violation of the FERPA, the Compliance Office recommends specific steps that the institution must take to comply. See 34 C.F.R. § 99.66. If the school fails to comply, then funding can be stopped.

**The Law Enforcement Exception.** Prior to a number of amendments in the 1990s, campus law enforcement records were covered by FERPA and therefore could not be disclosed to the public at large. In 1990, FERPA was amended to permit schools to inform violent crime victims of the results of school disciplinary proceedings. Pursuant to § 1232g(b)(6):

> Nothing in this section shall be construed to prohibit an institution of post-secondary education from disclosing, to an alleged victim of any crime of violence . . . the results of any disciplinary proceeding conducted by such institution against the alleged perpetrator of such crime with respect to such crime.4

A subsequent amendment to FERPA, in 1992, excluded from the definition of “education records” certain records created by an institution’s “law enforcement unit” at least in part for law enforcement purposes and maintained by that unit. § 1232g(a)(4)(B)(ii).

**Other Disclosure Exceptions.** Beyond the law enforcement exception, FERPA also contains other exceptions to its general prohibition against disclosure of education records. For example, it allows campus personnel to share information from records with other “school officials” who have legitimate educational interests” in the information. According to the Family Policy Compliance Office of the Department of Education, a legitimate educational interests exists when “the official needs to review an educational record in order to fulfill his or her professional responsibilities for the University.” In addition, FERPA contains an emergency exception for disclosure “to appropriate parties . . . if knowledge is necessary to protect the health or safety of the student or other individuals.”

p. 798 – Insert after note 1:

**2. FERPA and the Virginia Tech Shooter.** On April 16, 2007, Seung Cho, a student at Virginia Tech, shot and killed thirty-two students and faculty, wounded many others, and then took his own life. In the immediate aftermath of the tragedy, the Governor of Virginia appointed a panel to review the events leading up to the shootings and the handling of the incidents. Among other topics, the report looked at FERPA and other privacy laws.

The Review Panel found that many people knew about Cho’s mental insability yet they did not share what they knew with others because of widespread (and often incorrect) beliefs that information privacy laws blocked such information sharing:

While Cho was a student at Virginia Tech, his professors, fellow students, campus police, the Office of Judicial Affairs, the Care Team, and the Cook Counseling Center all had dealings with him that raised questions about his mental stability. There is no evidence that Cho’s parents
were ever told of these contacts, and they say they were unaware of his problems at school. Most significantly, there is no evidence that Cho’s parents, his suitemates, and their parents were ever informed that he had been temporarily detained, put through a commitment hearing for involuntary admission, and found to be a danger to himself. Efforts to share this information was impeded by laws about privacy of information, according to several university officials and the campus police. Indeed, the university’s attorney, during one of the panel’s open hearings and in private meetings, told the panel that the university could not share this information due to privacy laws.

The panel’s review of information privacy laws governing mental health, law enforcement, and educational records and information revealed widespread lack of understanding, conflicting practice, and laws that were poorly designed to accomplish their goals. Information privacy laws are intended to strike a balance between protecting privacy and allowing information sharing that is necessary or desirable. Because of this difficult balance, the laws are often complex and hard to understand.

The widespread perception is that information privacy laws make it difficult to respond effectively to troubled students. This perception is only partly correct. Privacy laws can block some attempts to share information, but even more often may cause holders of such information to default to the nondisclosure option—even when laws permit the option to disclose. Sometimes this is done out of ignorance of the law, and sometimes intentionally because it serves the purposes of the individual or organization to hide behind the privacy law. A narrow interpretation of the law is the least risky course, notwithstanding the harm that may be done to others if information is not shared.

Among other recommendations, the Report suggested:

The provisions [of privacy law] should insulate a person or organization from liability (or loss of funding) for making a disclosure with a good faith belief that the disclosure was necessary to protect the health, safety, or welfare of the person involved or members of the general public. Laws protecting good-faith disclosure for health, safety, and welfare can help combat any bias toward nondisclosure.65

What are the costs and benefits of this recommendation? Are there viable alternatives? How should officials share the mental health information of troubled students?

Regarding FERPA more specifically, the report noted that “FERPA does not address the differences between medical records and ordinary educational records such as grade transcripts. It is not clear whether FERPA preempts state law regarding medical records and confidentiality of medical information or merely adds another requirement on top of these records.” The report recommended that “FERPA should make explicit an exception regarding treatment records. Disclosure of treatment records from university clinics should be available to any health care provider without the student’s consent when the records are needed for medical treatment, as they would be if covered under HIPAA.” Additionally, the Report recommended that FERPA’s exception for release of records in an emergency should be interpreted more flexibly. The Report also recommended:

FERPA currently allows schools to release information in their records to parents who claim students as dependents. Schools are not, however, required to release that information. Yet, if a university adopts a policy against release to parents, it cuts off a vital source of information. The history of Seung Hui Cho shows the potential danger of such an approach. During his formative years, Cho’s parents worked with Fairfax County school officials, counselors, and outside mental health professionals to respond to episodes of unusual behavior. Cho’s parents told the panel that

had they been aware of his behavioral problems and the concerns of Virginia Tech police and educators about these problems, they would again have become involved in seeking treatment. The people treating and evaluating Cho would likely have learned something (but not all) of his prior mental health history and would have obtained a great deal of information germane to their evaluation and treatment of him. There is no evidence that officials at Virginia Tech consciously decided not to inform Cho’s parents of his behavior; regardless of intent, however, they did not do so. The example demonstrates why it may be unwise for an institution to adopt a policy barring release of information to parents.

Do you agree with these recommendations?

What kind of access should parents be allowed to information about their children once they are students at college? The Wall Street Journal has noted that MIT, for example, refused a mother access in April 2007 to her son's dorm room or to his computer's files after the twenty-two year old went missing. The student was shortly thereafter found drowned, a death that was considered a suicide. The mother managed to get into the dorm room, nonetheless, and to examine his computers. Some of the student's friends said her behavior, including going through his instant-messages conversations, made them feel uncomfortable. A MIT official commented, “Different students will do different things that they absolutely don't want their parents to know about.”

C. PRIVACY AT WORK

6. EMPLOYER MONITORING OF THE TELEPHONE

p. 851 – Add the following after Deal v. Spears; renumber subsequent notes:

1. Epilogue. Following the court’s decision, a number of other plaintiffs who were speaking with Deal while the conversations were being wiretapped filed suit. Each new plaintiff sought damages of $10,000 and attorneys fees and costs. The court, however, declined to award damages, noting 18 U.S.C. § 2520(c)(2) provides that “the court may assess . . . statutory damages of . . . $10,000.” Damages were thus at the discretion of the court, and the judge reasoned:

[T]he plaintiffs suffered no actual damages; the privacy intrusion as to these plaintiffs appears to have been relatively minor as compared to the intrusion into the affairs of Sibbie and Calvin Lucas; the Spears have already paid approximately $60,000.00 for their unlawful acts; the Spears, who are now retired and in their seventies, have no source of income other than their accumulated wealth; and Newell Spears used the recorder solely for the purpose of discovering who robbed his business. Though the court notes that the Spears’ accumulated wealth is substantial and would allow them to pay a significant judgment, this factor is outweighed by the others listed above, all of which counsel against an award of damages.


4. A Duty to Monitor Employees? In Doe v. XYC Corp., 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005), XYC Corporation employed Jane Doe’s husband as an accountant. The network administrator discovered that the employee was visiting porn sites. The employee’s supervisors told him to stop, and the employee said he would. The employee, however, had been videotaping and photographing his ten-year-old stepdaughter, Jill Doe, in the nude and transmitted three pictures of Jill Doe from his workplace computer to gain access to a child porn website. Jane Doe sued XYC on behalf of Jill, alleging that it knew or should have known that her husband was using his computer to view child porn and that it had a duty to report the employee to the authorities. XYC moved for summary judgment, but the court sided with the plaintiff:

We hold that an employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee’s activities and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third parties. No privacy interest of the employee stands in the way of this duty on the part of the employer. . . .

In this case, defendant had an e-mail policy which stated that “all messages composed, sent or received on the e-mail system are and remain the property of the [defendant]. They are not the private property of any employee.” Further, defendant reserved the “right to review, audit, access and disclose all messages created, received or sent over the e-mail system as deemed necessary by and at the sole discretion of [defendant].” Concerning the internet, the policy stated that employees were permitted to “access sites, which are of a business nature only” and provided that:

Any employees who discover a violation of this policy shall notify personnel. Any employee who violates this policy or uses the electronic mail or Internet system for improper purposes shall be subject to discipline, up to and including discharge.

The written e-mail policy contained an acknowledgement page to be signed by each employee. While the record does not contain a copy of such acknowledgement signed by Employee, there is no suggestion that he was not aware of the company policy. In addition, as we have noted, Employee’s office, as with others in the same area, did not have a door and his computer screen was visible from the hallway, unless he took affirmative action to block it. Under those circumstances, we readily conclude that Employee had no legitimate expectation of privacy that would prevent his employer from accessing his computer to determine if he was using it to view adult or child pornography. As a result, we turn to whether defendant had reason to investigate Employee’s use of his computer. . . .

Viewed in a light favorable to plaintiff, defendant was on notice of Employee’s pornographic related computer activity by early 2000. By late March 2001, defendant had knowledge, through its supervisory personnel, that Employee had visited a variety of “porn sites” including one that suggested child pornography. Yet, despite being reported to high level management, no action was taken. A reasonable fact-finder could conclude that an appropriate investigation at that time would have revealed the extent of Employee’s activities and, presumably, would have led to action to shut down those activities. It is true, as defendant contends, that Employee could still have possibly utilized a computer elsewhere, such as at home or at a library, to transmit Jill’s photos. But that possibility does not negate proximate cause as a matter of law; it simply presents a contested issue for a jury.
Doe v. XYC Corp. suggests that if an employer has a policy of monitoring its employees’ computer use, then that employer is responsible for harm resulting from not monitoring or from not disciplining employees who are in violation of the policy. What incentives does this create for employers? Is this case likely to be followed in other jurisdictions?
CHAPTER 9:
INTERNATIONAL PRIVACY LAW

SUMMARY OF ADDITIONS TO CHAPTER

• In B.2(e) (ECHR Article 8- Privacy and Place), we added Copland v. U.K., a new European Court of Human Rights opinion concerning workplace monitoring of employees.

• In E.4 (Passenger Name Record (PNR) Data Transfers), we included excerpts from a 2007 PNR agreement between the European Union and the U.S. as well as notes that explore criticisms of this agreement.

B. THE PROTECTION OF PRIVACY IN EUROPE

1. Convergence or Divergence?

p. 878 – Add the following after note 4:

5. Why Do the Privacy Law Regimes in the EU and US Differ? Francesca Bignami contends that “[w]hen individual privacy in the age of information technology first became a policy problem, American policymakers were every bit as active as their European counterparts. In fact, a case can be made that European privacy law was influenced by American law and policy.” But then things changed. Why? Bignami offers a number of reasons, one of which is that the EU has different enforcement mechanisms than the US:

In the American case, the primary enforcers are individual litigants; in the European case, they are independent privacy agencies. This is consistent with broader patterns of regulation in the two legal systems: Americans litigate in court and Europeans negotiate with government agencies. The American choice, however, appears to have been particularly ill suited to the realities of information privacy in the work of government agencies. The injuries suffered by individuals--not to speak of the polity--when the government secretly undertakes a program like that for call records are generally not recognized by common law courts. . . . A government agency with the authority to investigate other agencies for privacy violations, to recommend changes if such violations are found, and, in the last resort, to impose an administrative sanction or to take an offending government official to court, is likely to be a better enforcer than private attorneys general.67

---

B. THE PROTECTION OF PRIVACY IN EUROPE
2. ECHR ARTICLE 8
(b) Privacy and Law Enforcement

p. 888 – Add the following after note 4:

4. The NSA Surveillance Program and EU Law. Recall the excerpt from James Whitman, arguing that European privacy law primarily protects dignity and American privacy law primarily protects liberty against the state. Compare Francesca Bignami who argues:

In Europe, a secret government data-mining program like the NSA’s would be clearly illegal. Why? To summarize the rather complicated analysis that follows, such a data-mining program would violate two different types of privacy guarantees—procedural and substantive. Procedurally, government data mining, even for national security ends, would have to be authorized by a public law or regulation that specified the purposes of the personal data processing and the limits on that data processing, to minimize the government’s interference with private life. Before the program could be enacted, an independent government body would have to be consulted and, while the program was in operation, that same government body would need to have oversight and enforcement powers.

Substantively, the reach of a European data-mining program would be narrower than that of the NSA call database. Although a spy agency might be allowed access to all call information held by national telecommunications providers, it would not be allowed to retain the personal data as long as the NSA has—over five years now. Furthermore, the type of analysis performed on the data, as well as the uses of the results of the analysis, would have to be carefully circumscribed. The government would be permitted to use only search terms, statistical models, mathematical algorithms, and other analytical processes designed to uncover serious threats. . . . A spy agency in Germany would be allowed to pass on to law enforcement the names of individuals obtained through such data-mining techniques only if those individuals were suspected of planning to commit, or having already committed, a serious offense, and only if sufficient reasons existed for entertaining that suspicion.

Another substantive difference would be the right, under European law, of individuals to check on their information. This right of access enables individuals to ensure that their information is factually correct and is being handled in accordance with the guarantees of privacy law. Finally, to switch the focus briefly from the government to the private sector, the same amount of call data in the hands of telecommunications providers would not have been available to a European government. Under European law, telecommunications companies are prohibited from retaining personal data in the same quantities and for the same length of time as is routine—and legal—in the American business world.

Bignami later takes issue with Whitman:

Whitman obscures an important aspect of European privacy law. True, European privacy law promotes interpersonal respect among individuals. But it also protects privacy against the state. And it is not always true, as Whitman argues, that “state action will raise American hackles much more often than European ones.” . . . [I]n the context of antiterrorism data mining, European law protects liberty interests more than American law. At least European spy agencies tell their citizens when their personal data is being collected and combined and, depending on the results, sent to the police for further action, a lot more than can be said for American spy agencies.

B. THE PROTECTION OF PRIVACY IN EUROPE
2. ECHR ARTICLE 8
(e) Privacy and Place

p. 900 – Add the following before Section 3:

COPLAND V. U.K.
ECHR, 03/07/07

The Facts

6. The applicant was born in 1950 and lives in Llanelli, Wales.
7. In 1991 the applicant was employed by Carmarthenshire College (“the College”). The College is a statutory body administered by the State and possessing powers under sections 18 and 19 of the Further and Higher Education Act 1992 relating to the provision of further and higher education.
8. In 1995 the applicant became the personal assistant to the College Principal (“CP”) and from the end of 1995 she was required to work closely with the newly appointed Deputy Principal (“DP”).
9. In about July 1998, whilst on annual leave, the applicant visited another campus of the College with a male director. She subsequently became aware that the DP had contacted that campus to enquire about her visit and understood that he was suggesting an improper relationship between her and the director.
10. During her employment, the applicant’s telephone, e-mail and internet usage were subjected to monitoring at the DP’s instigation. According to the Government, this monitoring took place in order to ascertain whether the applicant was making excessive use of College facilities for personal purposes. The Government stated that the monitoring of telephone usage consisted of analysis of the college telephone bills showing telephone numbers called, the dates and times of the calls and their length and cost. The applicant also believed that there had been detailed and comprehensive logging of the length of calls, the number of calls received and made and the telephone numbers of individuals calling her. She stated that on at least one occasion the DP became aware of the name of an individual with whom she had exchanged incoming and outgoing telephone calls. The Government submitted that the monitoring of telephone usage took place for a few months up to about 22 November 1999. The applicant contended that her telephone usage was monitored over a period of about 18 months until November 1999.
11. The applicant’s internet usage was also monitored by the DP. The Government accepted that this monitoring took the form of analysing the web sites visited, the times and dates of the visits to the web sites and their duration and that this monitoring took place from October to November 1999. The applicant did not comment on the manner in which her internet usage was monitored but submitted that it took place over a much longer period of time than the Government admit.
12. In November 1999 the applicant became aware that enquiries were being made into her use of e-mail at work when her step-daughter was contacted by the College and asked to supply information about e-mails that she had sent to the College. The
applicant wrote to the CP to ask whether there was a general investigation taking place or whether her e-mails only were being investigated. By an e-mail dated 24 November 1999 the CP advised the applicant that, whilst all e-mail activity was logged, the information department of the College was investigating only her e-mails, following a request by the DP.

13. The Government submitted that monitoring of e-mails took the form of analysis of e-mail addresses and dates and times at which e-mails were sent and that the monitoring occurred for a few months prior to 22 November 1999. According to the applicant the monitoring of e-mails occurred for at least six months from May 1999 to November 1999. She provided documentary evidence in the form of printouts detailing her e-mail usage from 14 May 1999 to 22 November 1999 which set out the date and time of e-mails sent from her e-mail account together with the recipients’ e-mail addresses. . . .

15. There was no policy in force at the College at the material time regarding the monitoring of telephone, e-mail or internet use by employees. . . .

The Law

39. The Court notes the Government’s acceptance that the College is a public body for whose acts it is responsible for the purposes of the Convention. Thus, it considers that in the present case the question to be analysed under Article 8 relates to the negative obligation on the State not to interfere with the private life and correspondence of the applicant and that no separate issue arises in relation to home or family life. . . .

41. According to the Court’s case-law, telephone calls from business premises are *prima facie* covered by the notions of “private life” and “correspondence” for the purposes of Article 8 § 1. . . . It follows logically that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal internet usage.

42. The applicant in the present case had been given no warning that her calls would be liable to monitoring, therefore she had a reasonable expectation as to the privacy of calls made from her work telephone. The same expectation should apply in relation to the applicant’s e-mail and internet usage.

43. The Court recalls that the use of information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an “integral element of the communications made by telephone” The mere fact that these data may have been legitimately obtained by the College, in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8. Moreover, storing of personal data relating to the private life of an individual also falls within the application of Article 8 § 1. Thus, it is irrelevant that the data held by the college were not disclosed or used against the applicant in disciplinary or other proceedings.

44. Accordingly, the Court considers that the collection and storage of personal information relating to the applicant’s telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8.

45. The Court recalls that it is well established in the case-law that the term “in
accordance with the law” implies - and this follows from the object and purpose of Article 8 - that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by Article 8 § 1. This is all the more so in areas such as the monitoring in question, in view of the lack of public scrutiny and the risk of misuse of power.

46. This expression not only requires compliance with domestic law, but also relates to the quality of that law, requiring it to be compatible with the rule of law. In order to fulfil the requirement of foreseeability, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures.

47. The Court is not convinced by the Government’s submission that the College was authorised under its statutory powers to do “anything necessary or expedient” for the purposes of providing higher and further education, and finds the argument unpersuasive. Moreover, the Government do not seek to argue that any provisions existed at the relevant time, either in general domestic law or in the governing instruments of the College, regulating the circumstances in which employers could monitor the use of telephone, e-mail and the internet by employees. Furthermore, it is clear that the Telecommunications (Lawful Business Practice) Regulations 2000 (adopted under the Regulation of Investigatory Powers Act 2000) which make such provision were not in force at the relevant time.

48. Accordingly, as there was no domestic law regulating monitoring at the relevant time, the interference in this case was not “in accordance with the law” as required by Article 8 § 2 of the Convention. The Court would not exclude that the monitoring of an employee’s use of a telephone, e-mail or internet at the place of work may be considered “necessary in a democratic society” in certain situations in pursuit of a legitimate aim. However, having regard to its above conclusion, it is not necessary to pronounce on that matter in the instant case.

49. There has therefore been a violation of Article 8 in this regard.

54. The Government submitted that the report presented by the applicant gave no indication that the stress complained of was caused by the facts giving rise to her complaint. Furthermore, as the Court had held in a number of cases relating to complaints involving the interception of the communications of suspected criminals by the police, in their view, a finding of a violation should in itself constitute sufficient just satisfaction. Moreover, since the conduct alleged consisted of monitoring and not interception, the nature of such interference was of a significantly lower order of seriousness than the cases mentioned above.

55. The Court notes the above cases cited by the Government, but recalls also that, in Halford, which concerned the interception of an employee’s private telephone calls by her employer, it awarded GBP 10,000 in respect of non-pecuniary damage. Making an assessment on an equitable basis in the present case, the Court awards the applicant EUR 3,000 in respect of non-pecuniary damage. 69

58. . . . Taking into account all the circumstances, it awards the applicant EUR 6,000 for legal costs and expenses, in addition to any VAT that may be payable.

FOR THESE REASONS, THE COURT UNANIMOUSLY

69 [Editors’ Note: 3,000 Euros were worth approximately 2,023 British Pounds (GBP) in spring 2007].
1.  *Holds* that there has been a violation of Article 8 of the Convention . . .

3.  *Holds*

   (a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts, to be converted into pounds sterling at the rate applicable at the time of settlement: (i) EUR 3,000 (three thousand euros) in respect of non-pecuniary damage; (ii) EUR 6,000 (six thousand euros) in respect of costs and expenses; (iii) any tax that may be chargeable on the above amounts. . . .

**NOTES & QUESTIONS**

1. *Content and Telecommunication Attributes.* In *Copland v. United Kingdom*, the ECHR found that monitoring by employers did not have to collect the content of communications to be actionable under Article 8. In *Copland*, the employer had examined the data and length of telephone conversations, the numbers dialed, and web sites visited. But how might employers engage in such monitoring consistent with Article 8? The ECHR indicates in *Copland* that it “would not exclude” that “the monitoring of an employee’s use of a telephone, e-mail or internet at the place of work may be considered ‘necessary in a democratic society’ in certain situations in pursuit of a legitimate aim?” In your judgment, what kind of workplace monitoring would be appropriate? Should it depend on the particular position that an employee holds in the workplace? Note as well that Copland had not been warned that her telephone calls and emails would be subject to monitoring. Moreover, at the time of the employer’s surveillance, there was no law in the U.K. to govern such behavior. How could an European firm craft a workplace monitoring policy that would comport with *Copland*?

2. *EU vs. US?* In an analysis of *Copland*, Fred Cate has argued that it “may further widen the gulf between U.S. and European data protection laws and create challenges for multinational businesses and other organizations operating in Europe.”

   In addition to *Copland*, Cate identifies other EU decisions that block employer monitoring of telephone and Internet usage— even monitoring to investigate suspected wrongdoing and carried out with proper notice and authorized by a specific law. Cate concludes that *Copland* is “a potent reminder of how far European law has moved in the direction of workplace privacy and how great a challenge this movement poses for U.S. and multinational entities.”

**D. PRIVACY PROTECTION IN OTHER COUNTRIES**

p. 929 -- Insert new section:

5. *ASIAN PACIFIC ECONOMIC COOPERATION PRIVACY FRAMEWORK*

   Asia-Pacific Economic Cooperation (APEC) is a cooperative of economies located along the Pacific Ocean. It includes the U.S., China, Japan, the Russian

---

70 Fred Cate, *European Court of Human Rights Expands Privacy Protections*, 11 American Society of International Law Insight (August 6, 2007).
Federation, China, Australia, New Zealand, Peru, Indonesia, Mexico, Singapore, Thailand, and Vietnam. Ministers of these countries adopted a privacy framework, based on the OECD Guidelines, on November 24, 2004 at a meeting in Santiago, Chile. Then U.S. Secretary of State Colin Powell stated, “The APEC Privacy Framework will establish a consistent approach to privacy across APEC member economies, while also avoiding the creation of unnecessary barriers to information flows.” The APEC privacy framework seeks to enable multinational businesses to implement uniform approaches to the use of personal data. It contains nine principles. These are: (1) preventing harm; (2) notice; (3) collection limitation; (4) use of personal information; (5) choice; (6) integrity; (7) security safeguards; (8) access and correction; and (9) accountability. See APEC, Privacy Framework, Nov. 2004.

APEC’s Cross Border Privacy Rules Working Party, led by Australia, is now working on a system to implement the APEC Privacy Framework on an international basis. The Cross Border Privacy Rules (CBPR) will permit a business to fill out an application before engaging in an international data transfer to demonstrate that its privacy practices matched APEC privacy principles. The CBPR would permit resolving violations of CBPR’s through government enforcement agencies as well as private bodies for achieving accountability.

E. INTERNATIONAL TRANSFERS OF DATA

2. ADEQUATE LEVEL OF PROTECTION UNDER THE EU DIRECTIVE

p. 958 – Insert new note after note 3 :

4. Binding Corporate Rules. In addition to Model Contract Clauses, the EU has approved the use of Binding Corporate Rules (BCR’s) as a means to meet the Directive’s “adequacy test.” BCR’s must be uniform throughout the corporate group, and be enforceable by the individual whose data is being transferred. In January 2007, the Article 29 Working Group released a recommendation on BCR’s.

As part of its recommendation, the Article 29 Group developed a standard application, a single form, intended to streamline the process of obtaining approval of a BCR by a European Data Protection Authority (DPA). Only a single copy of the form need to be filled out and submitted to a so-called ”lead DPA.” 71 The recommendation also proposes a multi-factor test for deciding which Member Nation’s DPA should be the lead one. The Article 29 Group adds, “The DPAs are not obligated to accept the choice that you make if they believe another DPA is more suitable to be lead DPA.” 72

---


72 Id.
E. INTERNATIONAL TRANSFERS OF DATA
4. PASSENGER NAME RECORD DATA TRANSFERS

p. 964 - Insert New Note 5 and renumber subsequent note:

5. Update on the PNR Controversy. On May 30, 2006, the European Court of Justice found the 2004 Agreement on PNR to be unlawful. The flaw in the agreement did not have to do with privacy law; rather, the Court decided that the agreement was carried out, as a jurisdictional manner, in a fashion that violated European Community law. The solution of the Council of the EU was to sign an identical agreement between the US and EU, but to place its jurisdictional claim on firmer footing in EU law.

In addition, a 2007 PNR Agreement with an accompanying DHS Letter of Interpretation was issued by the Council of the EU as a legislative act on July 19, 2007. The 2007 PNR Agreement, among its other aspects, seeks to shift the transfer of PNR data from European air carriers to a “push” system. Under this approach, the airlines send the information to DHS. At any earlier stage, the US had sought a “pull” system under which a US agency would have direct access to the data systems of European carriers located in Europe. As you read through the 2007 Agreement and the DHS Letter, compare it to the 2004 agreement regarding what has changed and what has remained the same.

AGREEMENT BETWEEN THE EUROPEAN UNION AND THE UNITED STATES OF AMERICA ON THE PROCESSING AND TRANSFER OF PASSENGER NAME RECORD (PNR) DATA BY AIR CARRIERS TO THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY (DHS)
(2007 PNR AGREEMENT)
Official Journal L 204, 04/08/2007 p. 18

THE EUROPEAN UNION and THE UNITED STATES OF AMERICA,

DESIRING to prevent and combat terrorism and transnational crime effectively as a means of protecting their respective democratic societies and common values,

RECOGNISING that information sharing is an essential component in the fight against terrorism and transnational crime and that in this context the use of PNR data is an important tool,

RECOGNISING that, in order to safeguard public security and for law enforcement purposes, rules should be laid down on the transfer of PNR data by air carriers to DHS,

RECOGNISING the importance of preventing and combating terrorism and related crimes, and other serious crimes that are transnational in nature, including organised...
crime, while respecting fundamental rights and freedoms, notably privacy,

RECOGNISING that U.S. and European privacy law and policy share a common basis and that any differences in the implementation of these principles should not present an obstacle to cooperation between the U.S. and the European Union (EU), . . .

AFFIRMING that this Agreement does not constitute a precedent for any future discussions or negotiations between the United States and the European Union, or between either of the Parties and any State regarding the processing and transfer of PNR or any other form of data, . . .

HAVE AGREED AS FOLLOWS:

(1) On the basis of the assurances in DHS’s letter explaining its safeguarding of PNR (the DHS letter), the European Union will ensure that air carriers operating passenger flights in foreign air transportation to or from the United States of America will make available PNR data contained in their reservation systems as required by DHS.

(2) DHS will immediately transition to a push system for the transmission of data by such air carriers no later than 1 January 2008 for all such air carriers that have implemented such a system that complies with DHS’s technical requirements. For those air carriers that do not implement such a system, the current systems shall remain in effect until the carriers have implemented a system that complies with DHS’s technical requirements. Accordingly, DHS will electronically access the PNR from air carriers’ reservation systems located within the territory of the Member States of the European Union until there is a satisfactory system in place allowing for the transmission of such data by the air carriers.

(3) DHS shall process PNR data received and treat data subjects concerned by such processing in accordance with applicable U.S. laws, constitutional requirements, and without unlawful discrimination, in particular on the basis of nationality and country of residence. The DHS’s letter sets forth these and other safeguards.

(4) DHS and the EU, will periodically review the implementation of this Agreement, the DHS letter, and U.S. and EU PNR policies and practices with a view to mutually assuring the effective operation and privacy protection of their systems.

(5) By this Agreement, DHS expects that it is not being asked to undertake data protection measures in its PNR system that are more stringent than those applied by European authorities for their domestic PNR systems. DHS does not ask European authorities to adopt data protection measures in their PNR systems that are more stringent than those applied by the U.S. for its PNR system. If its expectation is not met, DHS reserves the right to suspend relevant provisions of the DHS letter while conducting consultations with the EU with a view to reaching a prompt and satisfactory resolution. In the event that a PNR system is implemented in the European Union or in one or more of its Member States that requires air carriers to make available to authorities PNR data for
persons whose travel itinerary includes a flight to or from the European Union, DHS shall, strictly on the basis of reciprocity, actively promote the cooperation of the airlines within its jurisdiction.

(6) For the application of this Agreement, DHS is deemed to ensure an adequate level of protection for PNR data transferred from the European Union. Concomitantly, the EU will not interfere with relationships between the United States and third countries for the exchange of passenger information on data protection grounds.

(7) The U.S. and the EU will work with interested parties in the aviation industry to promote greater visibility for notices describing PNR systems (including redress and collection practices) to the travelling public and will encourage airlines to reference and incorporate these notices in the official contract of carriage.

(8) The exclusive remedy if the EU determines that the U.S. has breached this Agreement is the termination of this Agreement and the revocation of the adequacy determination referenced in paragraph 6. The exclusive remedy if the U.S. determines that the EU has breached this agreement is the termination of this Agreement and the revocation of the DHS letter.

(9) . . . This Agreement and any obligations thereunder will expire and cease to have effect seven years after the date of signature unless the parties mutually agree to replace it.

This Agreement is not intended to derogate from or amend the laws of the United States of America or the European Union or its Member States. This Agreement does not create or confer any right or benefit on any other person or entity, private or public. . . .

For the European Union
For the United States of America

U.S. LETTER TO THE EUROPEAN UNION

In response to the inquiry of the European Union and to reiterate the importance that the United States government places on the protection of individual privacy, this letter is intended to explain how the United States Department of Homeland Security (DHS) handles the collection, use and storage of Passenger Name Records (PNR). . . .

I. Purpose for which PNR is used:
DHS uses EU PNR strictly for the purpose of preventing and combating: (1) terrorism and related crimes; (2) other serious crimes, including organized crime, that are transnational in nature; and (3) flight from warrants or custody for crimes described above. PNR may be used where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law. DHS will advise the EU regarding the passage of any U.S. legislation
which materially affects the statements made in this letter.

II. Sharing of PNR:
DHS shares EU PNR data only for the purposes named in Article I.
DHS treats EU PNR data as sensitive and confidential in accordance with U.S. laws and, at its discretion, provides PNR data only to other domestic government authorities with law enforcement, public security, or counterterrorism functions, in support of counterterrorism, transnational crime and public security related cases (including threats, flights, individuals and routes of concern) they are examining or investigating, according to law, and pursuant to written understandings and U.S. law on the exchange of information between U.S. government authorities. Access shall be strictly and carefully limited to the cases described above in proportion to the nature of the case.

EU PNR data is only exchanged with other government authorities in third countries after consideration of the recipient’s intended use(s) and ability to protect the information. Apart from emergency circumstances, any such exchange of data occurs pursuant to express understandings between the parties that incorporate data privacy protections comparable to those applied to EU PNR by DHS, as described in the second paragraph of this article.

III. Types of information collected:
Most data elements contained in PNR data can be obtained by DHS upon examining an individual’s airline ticket and other travel documents pursuant to its normal border control authority, but the ability to receive this data electronically significantly enhances DHS’s ability to focus its resources on high risk concerns, thereby facilitating and safeguarding bona fide travel.

Types of EU PNR Collected:
1. PNR record locator code
2. Date of reservation/issue of ticket
3. Date(s) of intended travel
4. Name(s)
5. Available frequent flier and benefit information (i.e. free tickets, upgrades, etc.)
6. Other names on PNR, including number of travelers on PNR
7. All available contact information (including originator information)
8. All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)
9. Travel itinerary for specific PNR
10. Travel agency/travel agent
11. Code share information
12. Split/divided information
13. Travel status of passenger (including confirmations and check-in status)
14. Ticketing information, including ticket number, one-way tickets and Automated Ticket Fare Quote
15. All baggage information
16. Seat information, including seat number
17. General remarks including OSI, SSI and SSR information
18. Any collected APIS information
19. All historical changes to the PNR listed in numbers 1 to 18

To the extent that sensitive EU PNR data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual), as specified by the PNR codes and terms which DHS has identified in consultation with the European Commission, are included in the above types of EU PNR data, DHS employs an automated system which filters those sensitive PNR codes and terms and does not use this information. Unless the data is accessed for an exceptional case, as described in the next paragraph, DHS promptly deletes the sensitive EU PNR data.

If necessary, in an exceptional case where the life of a data subject or of others could be imperilled or seriously impaired, DHS officials may require and use information in EU PNR other than those listed above, including sensitive data. In that event, DHS will maintain a log of access to any sensitive data in EU PNR and will delete the data within 30 days once the purpose for which it has been accessed is accomplished and its retention is not required by law. DHS will provide notice normally within 48 hours to the European Commission (DG JLS) that such data, including sensitive data, has been accessed.

IV. Access and redress:
DHS has made a policy decision to extend administrative Privacy Act protections to PNR data stored in the ATS regardless of the nationality or country of residence of the data subject, including data that relates to European citizens. Consistent with U.S. law, DHS also maintains a system accessible by individuals, regardless of their nationality or country of residence, for providing redress to persons seeking information about or correction of PNR.

Furthermore, PNR furnished by or on behalf of an individual shall be disclosed to the individual in accordance with the U.S. Privacy Act and the U.S. Freedom of Information Act (FOIA). FOIA permits any person (regardless of nationality or country of residence) access to a U.S. federal agency’s records, except to the extent such records (or a portion thereof) are protected from disclosure by an applicable exemption under the FOIA. DHS does not disclose PNR data to the public, except to the data subjects or their agents in accordance with U.S. law.

V. Enforcement:
Administrative, civil, and criminal enforcement measures are available under U.S. law for violations of U.S. privacy rules and unauthorized disclosure of U.S. records.

VII. Data retention:
DHS retains EU PNR data in an active analytical database for seven years, after which time the data will be moved to dormant, non-operational status. Data in dormant status will be retained for eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security and only in response to an identifiable case, threat, or risk. We expect that EU PNR data shall be deleted at the end of this period; questions of whether and when to destroy PNR data collected in
accordance with this letter will be addressed by DHS and the EU as part of future
discussions. Data that is related to a specific case or investigation may be retained in an
active database until the case or investigation is archived. It is DHS’ intention to review
the effect of these retention rules on operations and investigations based on its experience
over the next seven years. DHS will discuss the results of this review with the EU. . . .

VIII. Transmission:

Given our recent negotiations, you understand that DHS is prepared to move as
expeditiously as possible to a ‘push’ system of transmitting PNR from airlines operating
flights between the EU and the U.S. to DHS. Thirteen airlines have already adopted this
approach. . . . The transition to a ‘push’ system, however, does not confer on airlines any
discretion to decide when, how or what data to push. That decision is conferred on DHS
by U.S. law.

Under normal circumstances DHS will receive an initial transmission of PNR data
72 hours before a scheduled departure and afterwards will receive updates as necessary to
ensure data accuracy. . . .

We trust that this explanation has been helpful to you in understanding how we
handle EU PNR data.

Sincerely,
Michael Chertoff
Secretary of Homeland Security

EUROPEAN UNION LETTER TO THE UNITED STATES

Thank you very much for your letter to the Council Presidency and the
Commission explaining how DHS handles PNR data.

The assurances explained in your letter provided to the European Union allow the
European Union to deem, for the purposes of the international agreement signed between
the United States and European Union on the processing and transfer of PNR in July
2007, that DHS ensures an adequate level of data protection. . . .

We look forward to working with you and the aviation industry to ensure that
passengers are informed about how governments may use their information.

Yours sincerely,
Luis Amado
President of the Council

NOTES & QUESTIONS

a resolution strongly criticizing the 2007 PNR agreement. 74 It was “concerned that the

---

74 European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America, P6_TA-
0347&language=EN.
DHS’s handling, collection, use and storage of PNR data is (sic.) not founded on a proper agreement, but only on nonbinding assurances that can be unilaterally changed by the DHS at any given moment and that do not confer any rights or benefits on any person or party.” It protested “the fact that the length of retention of PNR data will be extended from 3.5 years to 15 years.” Do you understand where this fifteen year figure comes from?

The European Parliament also pointed out that “the reduction in data fields from 34 to 19” was “largely cosmetic due to the merging and renaming of data fields instead of actual deletions.” Finally, it expressed its concern that “data will be kept for seven years in ‘active analytical databases,’ leading to a significant risk of massive profiling and data mining, which is incompatible with basic European principles and is a practice still under discussion in the US Congress.”

2. Criticisms of European Officials. Other concerns have been raised about the 2007 PNR agreement. Like the European Parliament, the Federal Data Protection Commissioner of German, Peter Schaar, criticized the extension of the time for which information could be stored.75 The European Data Protection Supervisor, Peter Hustinx, spoke of the “concept of ‘dormant’ data” as being “without legal precedent.”76 He also noted that the U.S. was trying “to avoid a binding agreement by exchange of letters,” and that data on EU citizens “will be readily accessible to a broad range of U.S. agencies and there is no limitation to what US authorities are allowed to do with the data.” In the UK Parliament, the House of Lords European Union Committee issued a report that objected to the ability of the US to amend the PNR agreement unilaterally.77

3. The Push System. The 2007 PNR Agreement reflects a desire to move to a “push” system. What is the framework that the 2007 PNR Agreement establishes for this approach for sharing PNR?

4. A Lack of Territorial Leverage? For Francesca Bignami, EU officers negotiated at a disadvantage:

[I]n the case of airline passenger data it does not appear that Europe has been able to exert much leverage over the United States . . . European airlines wish to do business wish the United States. To do so, they must land and deplane their passengers at U.S. airports. To enjoy this privilege, European carriers are forced to comply with the U.S. government’s requests for personal information. And Europe has few carrots or sticks to use in negotiating privacy guarantees for such information.78

Bignami also noted the difficulty of European data protection authorities suing

78 Francesca Bignami, European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining, 48 B.C. L. Rev. 609, 674 (2007).
national carriers ("difficult as a matter of domestic politics") or American airlines ("would risk triggering retaliation from the American side"). In contrast, she argues that where Europeans held a territorial advantage, in negotiations concerning U.S. access to information on transnational crime in Europol’s central database, more privacy guarantees were gained by the negotiators for Europe.