(Md. App. 1979); *Richfield Bank & Trust Co. v. Sjogren*, 244 N.W.2d 648 (Minn. 1976); *McGuire v. Shubert,* 722 A.2d 1087 (Pa. Super. 1998).

CHAPTER 9

CONSUMER DATA

CHAPTER OUTLINE

We live in a world where commercial entities collect and maintain extensive databases of personal information about individuals. These businesses amass this information for a myriad of purposes. One of their chief reasons for their interest in personal data is to enhance their ability to market products and services to people.

A burgeoning form of marketing today consists of behavioral marketing—examining the behavior patterns of consumers to target advertisements to them. Today's marketer can draw on a wealth of knowledge and insights about human behavior to maximize the effectiveness of advertising. Interactions on the Internet and with other digital platforms permit the creation of an immense trail of personal data, as almost everything that people do online can be tracked. Individuals can now be followed across different websites or digital media. Advertisements can be tailored to specific individuals.

Consumer data can be used for other purposes too. It can be used to make inferences about a person's trustworthiness or aptitude for a job. It can be used for background checks or to determine whether a person will be an easy or difficult customer to deal with. The government can access consumer data for use in criminal investigations, general profiling, or a broad-scale amassing of data.

This chapter explores how the law regulates the collection and use of consumer data.

A. THE U.S. SYSTEM OF CONSUMER DATA PRIVACY REGULATION

In the United States, myriad types of law, which form a complicated patchwork of regulation, regulate consumer data privacy. In some contexts, the law provides strong protections of privacy. In other contexts, the law provides minimal protections. And in a number of contexts, there is hardly any legal protection.

1. STRUCTURE

The Sectoral Approach. Consumer privacy in the United States is regulated by "sectoral" laws that focus on various sectors of the economy. Different laws regulate different industries. In contrast to the United States, Europe and many other countries have an "omnibus" approach toward regulating privacy. Under an omnibus approach, one overarching statute regulates personal information use irrespective of the entities or industry that wishes to process the information. These general laws are frequently then supplemented in European countries and elsewhere outside of the United States by more targeted, sectoral laws. The "omnibus" law provides a general safety-net in these countries for areas or regulatory issues that a sectoral statute may not address.

The sectoral approach in the United States can sometimes draw even finer distinctions for similar kinds of information. For example, cable TV records are regulated differently from video rental or sale records. There are no industry-specific federal statutes directed towards the personal information contained in

records of most merchants (bookstores, supermarkets, clothing stores, electronics stories, etc.).

Self-Regulation. Self-regulation has formed a key foundation for U.S. consumer privacy law. As businesses began offering their products and services on the Internet in the 1990s, they operated in a realm that was largely unregulated. To ease concerns of consumers and to demonstrate that they could regulate themselves, businesses began to post privacy policies on their websites. These policies describe the information that is collected, how it will be used and shared, and how it will be safeguarded. Consumers are sometimes offered a choice to opt-out of some uses of their data.

Although privacy regulation has proliferated, some industries still lack a sectoral law. Privacy regulation also tends to allow businesses great flexibility in how they collect, use, or disclose personal data. Most companies use an approach called "notice and choice." They provide a privacy policy (sometimes called a "privacy notice") that describes the ways in which personal data will be collected, used, or disclosed. Consumers are then considered to have a choice. They can accept these terms and do business with the company, or they can refrain from doing business with the company. Sometimes companies offer choices to consumers regarding specific uses or disclosures of their information. Consumers may be given the ability to "opt in" or "opt out" of certain uses or disclosures. An "opt out" means that a consumer's information will be processed unless she takes action to contact the data processing entity and indicate her contrary wishes.

Since the late 1990s, the Federal Trade Commission (FTC) has deemed violations of privacy policies to be an "unfair or deceptive" practice under the FTC Act. The FTC has the power to enforce the FTC Act. The result of the FTC's involvement has been to create a system of quasi-self-regulation, where companies define the substantive terms of how they will collect, use, and disclose personal data, but they are then held accountable to these terms by the FTC. Over time, however, the FTC has interpreted the FTC Act as requiring more of companies than merely following promises.

The Chief Privacy Officer. Over the last two decades, there has been a significant rise in the number of "privacy professionals." The association for such individuals — the International Association of Privacy Professionals (IAPP) — has grown at rates from 30 percent to 40 percent. Beyond the large membership of this organization, a further indication of the ongoing development and specialization of privacy work is provided by the three certification titles that the IAPP grants. By taking examinations, an applicant can become a Certified Information Privacy Professional (CIPP), a Certified Information Privacy Manager (CIPM), or a Certified Information Privacy Technologist (CIPT).

Many companies have a chief privacy officer (CPO) who, among other things, develops a "privacy program" within an institution.[1] A privacy program typically has both elements involving compliance and strategy. Compliance means

[1] For two practitioner-oriented guides to the role of a CPO, see Michelle Finneran Dennedy et al., *The Privacy Engineer's Manifesto* (2014); *Building a Privacy Program* (Kirk M. Herath ed., 2011).

developing safeguards, including training the workface, to make sure that the company follows all privacy and security laws and regulations. Strategy means assessing privacy risks, training the workforce about privacy awareness, helping to shape products and services so that they minimize any potential privacy concerns, and stopping or limiting a company's actions that consumers might find too privacy-invasive. The CPO often helps manage not only the information companies have about consumers but also the data maintained about the workforce.

In some industries, laws or regulations require that companies have a designated employee to handle privacy and security responsibilities. An example would be the FTC's Safeguards Rule, issued pursuant to the Gramm-Leach-Bliley Act, which requires the designation of one employee at the covered entity to manage the company's responsibilities pursuant to the Rule. In other industries, businesses voluntarily have CPOs. In such companies, the rise of the CPO is tied to an increase of privacy and security obligations, whether through statutes, regulations, or contracts. As a consequence, it is efficient for a company to have a specialized employee to do this work. CPOs are now common in most large and medium-sized businesses.

As Kenneth Bamberger and Deirdre Mulligan note, "[C]orporate privacy management in the United States has undergone a profound transformation."[2] Based on a series of interviews with leading CPOs, Bamberger and Mulligan present an account of "privacy on the ground." In their view, these firms, driven by the leadership of CPOs, have adopted a dynamic approach to privacy issues. The approach "stressed the importance of integrating practices into corporate decision-making that would prevent the violation of consumer expectations." The respondent CPOs also emphasized the importance of developing "company law," by which they meant "consistent and coordinated firm-specific global privacy policies intended to ensure that a firm both complies with the requirements of all relevant jurisdictions and acts concordantly when dealing with additional business issues not governed by any particular regulation."

2. TYPES OF LAW

Tort Law. Tort law has been used by plaintiffs in response to various forms of data collection, use, or disclosure. Plaintiffs have attempted to use the Warren and Brandeis privacy torts, which were originally developed to address issues involving privacy and the media, as well as other torts, such as negligence. Later in this chapter we will explore how these attempts have fared.

Contract Law. In many instances, companies have a privacy policy that specifies how that information is to be collected, used, or disclosed. Later in this chapter we will explore whether these policies can be enforced as contracts or via promissory estoppel.

[2] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247, 251 (2011).

Property Law. Some commentators argue that personal data should be treated akin to property. If businesses want to collect or use it in certain ways, they must buy it from the individual, or otherwise trade for it. Later in this chapter we will explore whether treating personal data this way will result in the appropriate forms of data protection.

FTC Section 5 Enforcement. Since the mid-1990s, the Federal Trade Commission (FTC) has used Section 5 of the FTC Act to regulate consumer privacy. Section 5 prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45. The FTC views violations of privacy policies as a "deceptive" practice. It views a number of other practices as "unfair." The FTC's Section 5 jurisdiction is quite broad and encompasses most industries (except for a few carve outs). As a result, it has become the dominant agency regulating privacy in the United States. We will explore the FTC's enforcement of Section 5 later in this chapter.

Federal Statutory Regulation. There are numerous federal statutes pertaining to consumer privacy. As discussed above, the United States follows a sectoral approach to privacy regulation, so statutes differ in different industries and some industries lack their own law. The federal statutes will be discussed later in this chapter.

State Statutory Regulation. Many states have passed sectoral legislation regulating business records and databases. These state statutes sometimes have stronger protections of privacy than federal statutes. There are thousands of state statutes involving privacy, and because there are so many, this chapter focuses primarily on the federal statutes.

State statutes play a key role in the protection of privacy — even beyond the borders of a particular state. For example, California has passed a series of strong privacy protections, and, as a general matter, California can be said to have the strongest privacy law in the United States.[3] These statutes typically protect the personal data of California residents regardless of where the data processing occurs. Many companies have a segment of their business involving customers from California, which is not surprising because this state would be the world's eighth largest economy if it were a stand-alone country. Thus, these companies must comply with California's privacy laws for their customers based in this economically important state. Some companies carve out different policies and procedures to deal with California law, but others just follow California law for all customers because it is easier to follow just one set of rules, and California's laws are often the strictest.

The list of California privacy laws is extensive. California passed the first data breach notification law in 2002, and 46 states have now followed suit. One of California's more unique consumer privacy protections is its "Shine the Light" law. Passed in 2003, SB27, Cal. Civ. Code § 1798.83, allows consumers to obtain from businesses information about the personal data that the businesses disclosed

[3] The California Office of Privacy Protection maintains a comprehensive summary of California's privacy statutes: http://www.privacy.ca.gov/lawenforcement/laws.htm.

to third parties for direct marketing purposes. People can find out the kinds of personal information that a company provided to third parties for direct marketing purposes as well as the "names and addresses of all of the third parties that received personal information from the business." § 1798.83(1). The law applies to businesses with 20 or more employees. § 1798(c)(1). Companies with privacy policies that allow people to opt out of sharing of their data with third parties are exempt. § 1798(c)(2).

Other California privacy laws include an obligation placed on rental car companies to inform customers if they have a "black box" in their vehicles; the Confidentiality of Medical Information Act (CMIA), which is a general health information privacy law for the state; and the Song-Beverly Credit Card Act, discussed below, which limits the kinds of personal information collected by companies that accept credit cards.

NOTES & QUESTIONS

1. ***The Case for Less Privacy Regulation.*** Several commentators argue that self-regulation is preferable to creating more state and federal privacy laws. Fred Cate points out that self-regulation is "more flexible and more sensitive to specific contexts and therefore allow[s] individuals to determine a more tailored balance between information uses and privacy than privacy laws do."[4]

Eric Goldman argues:

> Relatively few consumers have bought privacy management tools, such as software to browse anonymously and manage Internet cookies and e-mail. Many vendors are now migrating away from consumer-centric business models. So, although consumers can take technological control over their own situation, few consumers do.
>
> Plus, as most online marketers know, people will "sell" their personal data incredibly cheaply. As Internet pundit Esther Dyson has said: "You do a survey, and consumers say they are very concerned about their privacy. Then you offer them a discount on a book, and they'll tell you everything." Indeed, a recent Jupiter report said that 82% of respondents would give personal information to new shopping sites to enter a $100 sweepstakes.
>
> Clearly consumers' stated privacy concerns diverge from what consumers do. Two theories might explain the divergence.
>
> First, asking consumers what they care about reveals only whether they value privacy. That's half the equation. Of more interest is how much consumers will pay — in time or money — for the corresponding benefits. For now, the cost-benefit ratio is tilted too high for consumers to spend much time or money on privacy.
>
> Second, consumers don't have uniform interests. Regarding online privacy, consumers can be segmented into two groups: activists, who actively protect their online privacy, and apathetics, who do little or nothing to protect themselves. The activists are very vocal but appear to be a tiny market segment.
>
> Using consumer segmentation, the analytical defect of broad-based online privacy regulations becomes apparent. The activists, by definition, take care of themselves. They demand privacy protections from businesses and, if they don't get it, use technology to protect themselves or take their business elsewhere.
>
> In contrast, mainstream consumers don't change their behavior based on online privacy concerns. If these people won't take even minimal steps to protect themselves, why should government regulation do it for them?
>
> Further, online businesses will invest in privacy when it's profitable. . . . When companies believed that few consumers would change their behavior if they were offered greater privacy, those companies did nothing or put into place privacy policies that disabused consumers of privacy expectations. Of course, if companies later discovered that they were losing business because customers wanted more privacy, they would increase their privacy initiatives.
>
> Consumer behavior will tell companies what level of privacy to provide. Let the market continue unimpeded rather than chase phantom consumer fears through unnecessary regulation.[5]

[4] Fred H. Cate, *Privacy in Perspective* 26 (2001); *see also* Fred H. Cate, *Privacy in the Information Age* (1997).

In contrast, Peter Swire contends that privacy legislation need not be antithetical to business interests. According to Swire, privacy legislation should be viewed as similar to the "trustwrap" that Johnson & Johnson placed around bottles of Tylenol after a scare involving cyanide poisoning of the pain reliever.[6] Swire believes that "privacy legislation targeted at online practices" would provide the kind of safety to allow consumers to engage in cyberspace activities with confidence.

2. ***Flexible Regulation.*** Some commentators contend that a middle ground can be found between traditional legal regulation and self-regulation. Dennis Hirsch argues that environmental law suggests ways to regulate privacy that are flexible and that mix legal regulation with self-regulation:

> Over the past forty years, environmental law has been at the epicenter of an intense and productive debate about the most effective way to regulate. Initial environmental laws took the form of prescriptive, uniform standards that have come to be known as "command-and-control" regulation. These methods, while effective in some settings, proved costly and controversial. In the decades that followed, governments, academics, environmental and business groups, and others poured tremendous resources into figuring out how to improve upon these methods. This work has produced a "second generation" of environmental regulation. . . .
>
> Second generation initiatives encourage the regulated parties themselves to choose the means by which they will achieve environmental performance goals. That is what defines them and distinguishes them from first generation regulations under which the agency has the primary decision-making power over pollution control methods. This difference tends to make second generation strategies more cost-effective and adaptable than command-and-control rules. The proliferation of second generation strategies has led some to identify the environmental field as having "some of the most innovative regulatory instruments in all of American law."
>
> Privacy regulation today finds itself in a debate similar to the one that the environmental field has been engaged in for years. On the one hand, there is a

[5] Eric Goldman, *The Privacy Hoax,* Forbes (Oct. 14, 2002), available at http://www.ericgoldman.org/Articles/privacyhoax.htm.

[6] Peter P. Swire, *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy*, 54 Hastings L.J. 847 (2003).

growing sense that the digital age is causing unprecedented damage to privacy and that action must be taken immediately to mitigate these injuries. On the other, a chorus of voices warns against the dangers of imposing intrusive and costly regulation on the emerging business sectors of the information economy. Missing thus far from the dialogue is any significant discussion of the more flexible "second generation" regulatory strategies that might be able to bridge this gap. It took environmental law decades to arrive at these alternatives. The privacy field could capitalize on this experience by looking to these environmental policies as models for privacy regulation.[7]

Is the analogy of privacy law to environmental law an apt one? To what extent are the privacy statutes discussed in this book thus far command-and-control rules versus flexible rules? Is Hirsch calling less for self-regulation than for industry input into the form and content of rules?

3. ***Is Privacy Still Possible?*** Is privacy still possible in an Information Age? Scott McNealy, CEO of Sun Microsystems, Inc., once remarked: "You already have zero privacy. Get over it." Should we eulogize the death of privacy and move on? Or is it possible to protect privacy in modern times?

   Consider David Brin:

> . . . [I]t is already far too late to prevent the invasion of cameras and databases. The *djinn* cannot be crammed back into its bottle. No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases. They are here to stay.
>
> Light *is* going to shine into nearly every corner of our lives. . . .
>
> If neo-Western civilization has one great trick in its repertoire, a technique more responsible than any other for its success, that trick is *accountability*. Especially the knack — which no other culture ever mastered — of making accountability apply to the mighty. . . .
>
> Kevin Kelly, executive editor of *Wired* magazine, expressed the same idea with the gritty clarity of information-age journalism: "The answer to the whole privacy question is more knowledge. More knowledge about who's watching you. More knowledge about the information that flows between us — particularly the meta-information about who knows what and where it's going."
>
> In other words, we may not be able to eliminate the intrusive glare shining on citizens of the next century, but the glare just might be rendered harmless through the application of more light aimed in the other direction.[8]

Is greater transparency the solution to the increasing threats to privacy?

4. ***Privacy Enhancing Technologies and Privacy by Design.*** As part of the self-governance, technology can assist companies as well as consumers in making privacy choices. Privacy on the Internet can be protected by another form of regulatory mechanism — technology. According to Joel Reidenberg, "law and government regulation are not the only source of rule-making. Technological capabilities and system design choices impose rules on participants."[9]

[7] Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 Ga. L. Rev. 1, 8-10 (2006).

[8] David Brin, *The Transparent Society* 8-23 (1998).

[9] Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 Tex. L. Rev. 553 (1998).

Reidenberg calls such forms of technological governance "Lex Informatica." In *Code*, Lawrence Lessig developed similar ideas, as expressed in his famous adage: code is law.[10] By that he means that a central fashion in which regulation takes place in cyberspace is through technological configurations and system design choice.[11]

In the privacy context, Privacy Enhancing Technologies (PETs) have received much attention from scholars and the privacy policy community. Herbert Burkert describes PETs as "technical and organizational concepts that aim at protecting personal identity. These concepts usually involve encryption in the form digital signatures, blind signature or digital pseudonyms."[12]

Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada, has coined the term "privacy by design," a related concept to PETs. According to Cavoukian, "*Privacy by Design* refers to the philosophy and approach of embedding privacy into the design, operation and management of information technologies and systems, across the entire information life cycle."[13]

Ira Rubinstein has developed a useful taxonomy of PETs as either "substitute PETs" or "complementary PETs."[14] In his definition, "[s]ubstitute PETs seek to protect privacy by ensuring that little or no personal data is collected in the first place, thereby making legal protections superfluous." As an example, Rubinstein points to client-centric architecture, such as the Tor network, that prevents or minimizes the collection of personal data by permitting anonymous browsing. He also notes that in "practice, many substitute PETs are more theoretical than practical" with few being widely deployed.

In contrast, complementary PETs are designed to implement legislative privacy principles or related legal requirements. Here, Rubinstein draws a further distinction and identifies two types of complementary PETs. First, there are "privacy-friendly PETs," which give people more control over their personal data through improved notice and consent mechanisms, browser management tools, and dashboard interfaces. Second, "privacy-preserving PETs" resemble substitute PETs in that they rely on technology to limit data collection while also complementing legal requirements. Rubinstein's examples of this final category are privacy-preserving data mining and privacy-preserving targeted advertising. He concludes by arguing that "the market incentives for substitute PETs are feeble" and that "regulatory incentives may still be necessary to overcome the reluctance of private firms to increase their investments in PETs, especially in the face of limited consumer demand, competing business needs, and a weak economy."

[10] Larry Lessig, Code and Other Laws of Cyberspace (1999).

[11] For an analysis of Lessig's suggestions for privacy, see Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy*, 2000 Wisc. L. Rev. 743.

[12] Herbert Burkert, Privacy-Enhancing Technologies: Typology, Critique, Vision, in Technology and Privacy: The New Landscape 123, 125, 128 (Philip E. Agre & Marc Rotenberg, eds., 1997).

[13] Ann Cavoukian, Privacy by Design Resolution (2010), http://www.ipc.on.ca/site_documents/pbd-resolution.pdf.

[14] Ira S. Rubinstein, *Regulating Privacy by Design*, 26 Berkeley Tech. L.J. 1409 (2012).

Additionally, Rubinstein contrasts PETs with privacy by design. Whereas most PETs are "added-on to existing systems, sometimes as an afterthought by designers and sometimes by privacy-sensitive end-users," privacy by design is a systematic approach to developing any product or service "that embeds privacy into the underlying specifications or architecture." Although this approach has great potential, Rubinstein suggests that in order for privacy by design to achieve greater success than PETs, governments will have to clarify what it means for companies to "build in" privacy from the outset rather than "bolt it on" at the end and create regulatory incentives that will spur broader adoption.

3. PERSONALLY IDENTIFIABLE INFORMATION (PII)

PII is one of the most central concepts in privacy regulation. It defines the scope and boundaries of a large range of privacy statutes and regulations. Federal statutes that turn on this distinction include the Children's Online Privacy Protection Act, the Gramm-Leach-Bliley Act, the HITECH Act, and the Video Privacy Protection Act. Moreover, state statutes that rely on PII as a jurisdictional trigger include California's Song-Beverly Credit Card Act and the many data security breach notification laws. These laws all share the same basic assumption—that in the absence of PII, there is no privacy harm. Thus, privacy regulation focuses on the collection, use, and disclosure of PII and leaves non-PII unregulated.

Given PII's importance, it is surprising that information privacy law in the United States lacks a uniform definition of the term. Computer science has also shown that the very concept of PII is far from straightforward. Increasingly, technologists can take information that appears on its face to be non-identifiable and turn it into identifiable data. Instead of defining PII in a coherent and consistent manner, privacy law offers multiple competing definitions, each with some significant problems and limitations.

Approaches to PII. There are three predominant approaches to defining PII in various laws and regulations: (1) the "tautological" approach, (2) the "non-public" approach, and (3) the "specific-types" approach.[15] These approaches are also made either as a rule or standard. A standard is an open-ended decision-making yardstick, and a rule, its counterpart, is a harder-edged decision-making tool.

The tautological approach defines PII as any information that identifies a person. The Video Privacy Protection Act (VPPA) demonstrates this model. The VPPA, which safeguards the privacy of video sales and rentals, simply defines "personally identifiable information" as "information which identifies a person." One problem with this approach is that it simply states that PII is PII without providing guidance about how to identify PII.

[15] Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information,* 86 N.Y.U. L. Rev. 1815 (2011). For an analysis of concepts of personal information in the European Union, see Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the U.S. and EU*, 102 Cal. L. Rev. 877 (2014).

A second approach toward defining PII focuses on non-public information. The Gramm-Leach-Bliley Act (GLB Act) epitomizes this approach by defining "personally identifiable financial information" as "nonpublic personal information." The statute fails to define "nonpublic," but presumably this term means information not found within the public domain. The non-public approach, however, does not map onto whether the information is in fact identifiable.

The third approach is to list specific types of data that constitute PII. In the context of the specific-types approach, if the information falls into an enumerated group, it becomes a kind of statutory "per se" PII. The federal Children's Online Privacy Protection Act (COPPA) of 1998 illustrates this approach. COPPA states that personal information is "individually identifiable information about an individual collected online" that includes a number of elements beginning with "first and last name," and continuing through a physical address, Social Security number, telephone number, and e-mail address. Its definition of PII also includes "any other identifier that the [Federal Trade Commission (FTC)] determines permits the physical or online contacting of a specific individual." A limitation with the specific-types approach is that it can fail to respond to new technology, which is capable of transforming the kinds of data that are PII.

State privacy laws also define personal information. One of the most important of these laws is the Song-Beverly Credit Card Act, which prevents business from requesting "personal identification information" during credit card transactions. This statute has been the object of considerable litigation. In *Pineda v. Williams-Sonoma Stores* (2011), the California Supreme Court evaluated whether a ZIP code was protection personal information under the Song-Beverly Act. In *Apple v. Krescent* (2013), the same court considered whether this law's prohibitions extended to online merchants offering products that were downloadable.

PINEDA V. WILLIAMS-SONOMA STORES

246 P.3d 162 (Cal. 2011)

MORENO, J. The Song-Beverly Credit Card Act of 1971 (Credit Card Act) (Civ. Code, § 1747 *et seq.*) is "designed to promote consumer protection." *Florez v. Linens 'N Things, Inc.*, 108 Cal. App. 4th 447, 450, (2003). One of its provisions, section 1747.08, prohibits businesses from requesting that cardholders provide "personal identification information" during credit card transactions, and then recording that information.

Plaintiff sued defendant retailer, asserting a violation of the Credit Card Act. Plaintiff alleges that while she was paying for a purchase with her credit card in one of defendant's stores, the cashier asked plaintiff for her ZIP code. Believing it necessary to complete the transaction, plaintiff provided the requested information and the cashier recorded it. Plaintiff further alleges that defendant subsequently used her name and ZIP code to locate her home address.

We are now asked to resolve whether section 1747.08 is violated when a business requests and records a customer's ZIP code during a credit card transaction. In light of the statute's plain language, protective purpose, and legislative history, we conclude a ZIP code constitutes "personal identification

information" as that phrase is used in section 1747.08. Thus, requesting and recording a cardholder's ZIP code, without more, violates the Credit Card Act. We therefore reverse the contrary judgment of the Court of Appeal and remand for further proceedings consistent with our decision. . . .

Plaintiff visited one of [defendant Williams-Sonoma's] California stores and selected an item for purchase. She then went to the cashier to pay for the item with her credit card. The cashier asked plaintiff for her ZIP code and, believing she was required to provide the requested information to complete the transaction, plaintiff provided it. The cashier entered plaintiff's ZIP code into the electronic cash register and then completed the transaction. At the end of the transaction, defendant had plaintiff's credit card number, name, and ZIP code recorded in its database.

Defendant subsequently used customized computer software to perform reverse searches from databases that contain millions of names, e-mail addresses, telephone numbers, and street addresses, and that are indexed in a manner resembling a reverse telephone book. The software matched plaintiff's name and ZIP code with plaintiff's previously undisclosed address, giving defendant the information, which it now maintains in its own database. Defendant uses its database to market products to customers and may also sell the information it has compiled to other businesses. . . .

Section 1747.08, subdivision (a) provides, in pertinent part, "[N]o person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business shall . . . : (2) Request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to provide *personal identification information,* which the person, firm, partnership, association, or corporation accepting the credit card writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise. Subdivision (b) defines personal identification information as "information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number." Because we must accept as true plaintiff's allegation that defendant requested and then recorded her ZIP code, the outcome of this case hinges on whether a cardholder's ZIP code, without more, constitutes personal identification information within the meaning of section 1747.08. We hold that it does.

Subdivision (b) defines personal identification information as "information *concerning* the cardholder . . . including, but not limited to, the cardholder's address and telephone number" (italics added). "Concerning" is a broad term meaning "pertaining to; regarding; having relation to; [or] respecting. . . ." (Webster's New Internat. Dict. (2d ed. 1941) p. 552.) A cardholder's ZIP code, which refers to the area where a cardholder works or lives is certainly information that pertains to or regards the cardholder.

In nonetheless concluding the Legislature did not intend for a ZIP code, without more, to constitute personal identification information, the Court of Appeal pointed to the enumerated examples of such information in subdivision (b), i.e., "the cardholder's address and telephone number." . . . [T]he Court of Appeal reasoned that an address and telephone number are "specific in nature regarding an individual." By contrast, the court continued, a ZIP code pertains to the *group* of individuals who live within the ZIP code. Thus, the Court of Appeal concluded,

a ZIP code, without more, is unlike the other terms specifically identified in subdivision (b).

There are several problems with this reasoning. First, a ZIP code is readily understood to be part of an address; when one addresses a letter to another person, a ZIP code is always included. The question then is whether the Legislature, by providing that "personal identification information" includes "the cardholder's address" intended to include components of the address. The answer must be yes. Otherwise, a business could ask not just for a cardholder's ZIP code, but also for the cardholder's street and city in addition to the ZIP code, so long as it did not also ask for the house number. Such a construction would render the statute's protections hollow. Thus, the word "address" in the statute should be construed as encompassing not only a complete address, but also its components.

Second, the court's conclusion rests upon the assumption that a complete address and telephone number, unlike a ZIP code, are specific to an individual. That this assumption holds true in all, or even most, instances is doubtful. In the case of a cardholder's home address, for example, the information may pertain to a group of individuals living in the same household. Similarly, a home telephone number might well refer to more than one individual. The problem is even more evident in the case of a cardholder's *work* address or telephone number—such information could easily pertain to tens, hundreds, or even thousands of individuals. Of course, section 1747.08 explicitly provides that a cardholder's address and telephone number constitute personal identification information; that such information *might also* pertain to individuals other than the cardholder is immaterial. Similarly, that a cardholder's ZIP code pertains to individuals in addition to the cardholder does not render it dissimilar to an address or telephone number.

More significantly, the Court of Appeal ignores another reasonable interpretation of what the enumerated terms in section 1747.08, subdivision (b) have in common, that is, they both constitute information unnecessary to the sales transaction that, alone or together with other data such as a cardholder's name or credit card number, can be used for the retailer's business purposes. Under this reading, a cardholder's ZIP code is similar to his or her address or telephone number, in that a ZIP code is both unnecessary to the transaction and can be used, together with the cardholder's name, to locate his or her full address. The retailer can then, as plaintiff alleges defendant has done here, use the accumulated information for its own purposes or sell the information to other businesses.

There are several reasons to prefer this latter, broader interpretation over the one adopted by the Court of Appeal. The Court of Appeal's interpretation, by contrast, would permit retailers to obtain indirectly what they are clearly prohibited from obtaining directly, "end-running" the statute's clear purpose. This is so because information that can be permissibly obtained under the Court of Appeal's construction could easily be used to locate the cardholder's complete address or telephone number. Such an interpretation would vitiate the statute's effectiveness. . . .

[T]he legislative history of section 1747.08 offers additional evidence that plaintiff's construction is the correct one. . . .

Thus, in light of the statutory language, as well as the legislative history and evident purpose of the statute, we hold that personal identification information, as that term is used in section 1747.08, includes a cardholder's ZIP code.

APPLE V. KRESCENT

292 P.3d 883 (Cal. 2013)

LIU, J. The Song-Beverly Credit Card Act of 1971 (Credit Card Act) governs the issuance and use of credit cards. ([Cal.] Civ. Code, § 1747 *et seq.*). One of its provisions, section 1747.08, prohibits retailers from "[r]equest[ing], or requir[ing] as a condition to accepting the credit card as payment . . ., the cardholder to write any personal identification information upon the credit card transaction form or otherwise". . . . It also prohibits retailers from requesting or requiring the cardholder "to provide personal identification information, which the [retailer] . . . writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise," and from "[u]tiliz[ing] . . . a credit card form which contains preprinted spaces specifically designed for filling in any personal identification information of the cardholder." . . . .

We must resolve whether section 1747.08 prohibits an online retailer from requesting or requiring personal identification information from a customer as a condition to accepting a credit card as payment for an electronically downloadable product. Upon careful consideration of the statute's text, structure, and purpose, we hold that section 1747.08 does not apply to online purchases in which the product is downloaded electronically. . . .

Petitioner Apple Inc. (Apple), defendant below, operates an Internet Web site and an online iTunes store through which it sells digital media such as downloadable audio and video files. In June 2011, plaintiff below, David Krescent, sued Apple on behalf of himself and a putative class of similarly situated individuals for alleged violations of section 1747.08. Specifically, Krescent alleged that he purchased media downloads from Apple on various occasions and that, as a condition of receiving these downloads, he was required to provide his telephone number and address in order to complete his credit card purchase. He further alleged that Apple records each customer's personal information, is not contractually or legally obligated to collect a customer's telephone number or address in order to complete the credit card transaction, and does not require a customer's telephone number or address for any special purpose incidental but related to the individual credit card transaction, such as shipping or delivery. Although he alleged that "the credit card transaction would be permitted to proceed" without any personal identification information, Krescent also contended that "even if the credit card processing company or companies required a valid billing address and [credit card identification number], under no circumstance would [plaintiff's] telephone number be required to complete his transaction, that is, under no circumstance does [Apple] need [plaintiff's] phone number in order to complete a [media] download transaction.". . .

We review de novo questions of statutory construction. In doing so, "our fundamental task is to ascertain the intent of the lawmakers so as to effectuate the purpose of the statute." As always, we start with the language of the statute,

"giv[ing] the words their usual and ordinary meaning . . . while construing them in light of the statute as a whole and the statute's purpose." *Pineda v. Williams Sonoma,* 246 P.3d 612 (Cal. 2011). . . .

We begin with the text of the statute. Section 1747.08(a) provides: "Except as provided in subdivision (c), no person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business shall do any of the following: (1) Request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to write any personal identification information upon the credit card transaction form or otherwise. (2) Request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to provide personal identification information, which the person, firm, partnership, association, or corporation accepting the credit card writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise. (3) Utilize, in any credit card transaction, a credit card form which contains preprinted spaces specifically designated for filling in any personal identification information of the cardholder." Section 1747.08, subdivision (b) (hereafter section 1747.08(b)) defines "personal identification information" as "information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number." . . .

Although section 1747.08 does not explicitly reference online transactions, both parties maintain that the Legislature's intent is apparent from the plain meaning of the statute's terms. Krescent contends that the language of section 1747.08(a) "must be read as an all-inclusive prohibition on every businesses [sic] regardless of the form of the transaction." According to Krescent, in directing the statutory prohibition at any "person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business" (§ 1747.08(a)), the Legislature intended to include all retailers without exception. If the Legislature intended to exempt online retailers, he contends, it could have done so.

Apple, on the other hand, argues that the first sentence of section 1747.08(a) must be construed in light of other language in the statute indicating that the Legislature had in mind only in-person business transactions. For example, section 1747.08(a)(1) prohibits a retailer from requesting or requiring a "cardholder to *write* any personal identification information *upon the credit card transaction form* or otherwise." (Italics added.) Section 1747.08(a)(2) prohibits a retailer from requesting or requiring the cardholder to provide such information, which the retailer "*writes, causes to be written, or otherwise records upon the credit card transaction form* or otherwise." (Italics added.) And section 1747.08(a)(3) prohibits the retailer from utilizing "a *credit card form which contains preprinted spaces.*" (Italics added.) Apple says the terms "write" and "forms" imply, by their physicality, that section 1747.08 applies only to in-person transactions. Apple further argues that the definition of "credit card" in section 1747.02—"any card, plate, coupon book, or other single credit device existing for the purpose of being used from time to time *upon presentation* to obtain money, property, labor, or services on credit"—indicates that the Legislature contemplated only those transactions in which the card is physically presented or displayed to the retailer. (§ 1747.02, subd. (a), italics added.)

We think the text of section 1747.08(a) alone is not decisive on the question before us. The statutory language suggests that the Legislature, at the time it enacted former section 1747.8, did not contemplate commercial transactions conducted on the Internet. But it does not seem awkward or improper to describe the act of typing characters into a digital display as "writing" on a computerized "form." In construing statutes that predate their possible applicability to new technology, courts have not relied on wooden construction of their terms. Fidelity to legislative intent does not "make it impossible to apply a legal text to technologies that did not exist when the text was created. . . . Drafters of every era know that technological advances will proceed apace and that the rules they create will one day apply to all sorts of circumstances they could not possibly envision." (Scalia & Garner, *Reading Law: The Interpretation of Legal Texts* (2012). . . .

In this case . . . the plain meaning of the statutes text is not decisive. An examination of the statutory scheme as a whole is necessary to determine whether it is applicable to a transaction made possible by technology that the Legislature did not envision. . . .

We recently considered the history and purpose of the [Song-Beverly Act and determined that] "[t]he statute's overriding purpose was to "protect the personal privacy of consumers who pay for transactions with credit cards." (*Pineda,* 246 P.3d at 636). . . . Specifically, the Legislature "sought to address the misuse of personal identification information for, *inter alia*, marketing purposes, and found that there would be no legitimate need to obtain such information from credit card customers if it was not necessary to the completion of the credit card transaction." . . .

While it is clear that the Legislature enacted the Credit Card Act to protect consumer privacy, it is also clear that the Legislature did not intend to achieve privacy protection without regard to exposing consumers and retailers to undue risk of fraud. The legislative history shows that the Legislature enacted the statute's prohibitions only after carefully considering and rejecting the possibility that the collection of personal identification information by brick-and-mortar retailers could serve a legitimate purpose such as fraud prevention. In particular, the Senate Judiciary Committee considered the standard procedure followed by brick-and-mortar retailers in the 1990s to verify the identity of credit card users—which included "verify[ing] the identification of the cardholder by comparing the signature on the credit card transaction form with the signature on the back of the card" and "contact [ing] the credit card issuer's authorization center [to] obtain approval" for sales above a specified "floor limit"—and concluded that the collection of personal identification information was not a necessary step in that procedure. (Sen. Judiciary Com., Analysis of Assem. Bill No. 2920 (1989–1990 Reg. Sess.) as amended June 27, 1990, p. 3.) This finding supported the Legislature's judgment that brick-and-mortar retailers in the 1990s had no genuine need to collect personal identification information and would instead use such information primarily for unsolicited marketing. (See *id.* at pp. 3-4 [noting that the "problem" the bill was designed to address was retailers' practice of leading consumers "to mistakenly believe that [personal identification information] is a necessary condition to complete the credit card transaction, when, in fact, it is not" and "acquir[ing] this additional personal information for their own business purposes—for example, to build mailing or telephone lists which they can subsequently use for their own in-house marketing efforts, or sell to direct-mail or tele-marketing specialists, or to others"]; *id.* at pp. 5-7 [explaining that retailers had no genuine need for personal identification information to address problems such as billing errors, lost credit cards, and product problems].) We cannot assume that the Legislature, had it confronted a type of transaction in which the standard mechanisms for verifying a cardholder's identity were not available, would have made the same policy choice as it did with respect to transactions in which it found no tension between privacy protection and fraud prevention. . . .

The safeguards against fraud that are provided in section 1747.08(d) are not available to the online retailer selling an electronically downloadable product. Unlike a brick-and-mortar retailer, an online retailer cannot visually inspect the credit card, the signature on the back of the card, or the customer's photo identification. Thus, section 1747.08(d)—the key antifraud mechanism in the statutory scheme—has no practical application to online transactions involving electronically downloadable products. We cannot conclude that if the Legislature in 1990 had been prescient enough to anticipate online transactions involving electronically downloadable products, it would have intended section 1747.08(a) 's prohibitions to apply to such transactions despite the unavailability of section 1747.08 (d)'s safeguards.

Krescent's complaint reinforces our conclusion insofar as it failed to allege that Apple does not require any personal identification information to verify the identity of the credit card user. His complaint merely alleged that "the credit card transaction would be permitted to proceed without any further information" and that Apple "is not contractually obligated to provide a consumer's telephone number and/or address in order to complete the credit card transaction," thereby rendering inapplicable the exception set forth in section 1747.08(c)(3)(A). Even if credit card transactions may proceed without any personal identification information under the contractual terms that bind retailers and credit card companies, the fact remains that the Legislature saw fit to include section 1747.08(d) 's safeguards against fraud in the statutory scheme. The inclusion of section 1747.08(d), separate and apart from the exception in section 1747.08(c)(3)(A), reflects the Legislature's judgment that consumers and retailers have an interest in combating fraud that is independent of whatever security measures are (or are not) required by contracts between retailers and credit card issuers. Consistent with this legislative judgment, both parties acknowledged at oral argument that retailers often bear the risk of loss from fraudulent credit card charges. . . .

KENNARD, J. DISSENTING. . . . To protect consumer privacy, California statutory law prohibits retail sellers from recording the personal identification information, such as home addresses and telephone numbers, of their credit-card-using customers. Cal. Civ. Code § 1747.08, Subdiv. (a). The statute does not exempt online sales of downloadable products from this prohibition, and on its face the statute applies to sales conducted over the Internet just as it does to sales conducted face-to-face or by mail or telephone. Yet the majority holds that online sales of downloadable products are not covered by the statute, thus leaving Internet retailers free to demand personal identification information from their credit-card-using customers and to resell that information to others. The majority's

decision is a major win for these sellers, but a major loss for consumers, who in their online activities already face an ever-increasing encroachment upon their privacy.

Unlike the majority, I conclude that the statute means just what it says and contains no exemption, express or implied, for online sales of downloadable products. The majority's expressed concern that this plain-meaning construction of the statute leaves online sellers with no way to detect and prevent fraudulent purchases is unjustified. . . .

BAXTER, J. DISSENTING. . . . Section 1747.08 of the [Cal.] Civil Code was enacted to prevent any retailer such as defendant Apple Inc. from collecting and exploiting the personal identification information of consumers who use credit cards to make their purchases. Plaintiff's complaint sufficiently states a cause of action under this statute: it alleges that defendant required and recorded plaintiff's address and telephone number as a condition to his online purchases of electronically downloadable products, and that defendant's actions were not otherwise permitted by the statute. In holding to the contrary, the majority relies on speculation and debatable factual assumptions to carve out an expansive exception to section 1747.08 that leaves online retailers free to collect and use the personal identification information of credit card users as they wish. . . .

The majority implicitly agrees that defendant's conduct falls within the plain terms of section 1747.08(a). . . . The majority holds, however, that plaintiff was not entitled to protection of his personal identification information because online credit card purchases of electronically downloadable products are categorically exempt from the statute's application. . . . Although recognizing this is a question of statutory construction, the majority reaches a result that is contrary to the terms, purpose, and legislative history of section 1747.08. . . .

NOTES & QUESTIONS

1. **Pineda *and the "Specific Types" Approach to PII.*** The California Supreme Court reversed the lower courts in *Pineda*, but did so on the narrowest possible grounds. It analyzed the statutory language and legislative history, and found that both supported a legislative intent to include a ZIP code as part of the "cardholder's address." In other words, that statutory category included "not only a complete address, but its components."

   In a sense, the California Supreme Court in *Pineda* only tweaked a subcategory within the specific-types approach to defining PII. It did not reach the broader conclusion that the Song-Beverly Act reflected a policy to prevent retailers from collecting "identification" indices that would permit a definitive linkage between a customer and her address. In fact, the law can be read simply as a prohibition on merchants collecting information that is specific enough to allow the unique identification of a person. Although as many as tens of thousands of people might share a ZIP code, it was precisely the piece of information, when added to a person's name, which permitted linkage of the customer to a wealth of PII about her.

2. **Krescent *and Antifraud Considerations.*** Two years after *Pineda*, the California Supreme Court in *Krescent* decided that the overall statutory scheme of the Song-Beverly Act indicated a legislative desire to balance privacy protection and fraud protection. In particular, for electronically downloadable products, merchants faced limitations on their anti-fraud activities, which brick-and-mortar retailers did not. Ultimately, the California Supreme Court found that the legislature did not intend to have the relevant prohibitions in the Act extend to online merchants. How do you think the legislature should respond to this decision? Should online merchants be prevented from collecting telephone numbers and addresses from customers?
3. ***E-mailed Receipts, ZIP Codes, and Deposits.*** The Song-Beverly Act has led to litigation beyond *Pineda* and *Krescent*. For example, a federal court found that Nordstrom violated the act by requesting an e-mail address to mail a customer a receipt and then also using the e-mail to send the customer promotional communications and materials. Capp v. Nordstrom, 2013 WL 5739102 (E.D. Cal. 2013). The court found that an e-mail address was "personal identification information" under the Song-Beverly Act. It declared that a credit cardholder's e-mail address was an even "more specific and personal" reference to the person than the ZIP code at stake in *Pineda*. It stated, "Instead of referring to the general area in which a cardholder lives or works, a cardholder's email address permits direct contact and implicates the privacy interests of a cardholder."

   The Ninth Circuit has also considered whether the Song-Beverly Act prevented Redbox, a self-service kiosk used to rent movies and video games, from collecting ZIP codes. Sinibaldi v. Redbox Automated Retail, 754 F.3d 703 (9th Cir. 2014). The Ninth Circuit noted that the Song-Beverly Act contained a specific exemption where "the credit card is being used as a deposit to secure payment in the event of default, loss, damage, or similar occurrence." Cal. Civ. Code 1747.08(c)(1). While Redbox's request for the ZIP code was one for "personal identification information" under the Song-Beverly Act, it was collecting this information along with the credit card number as a deposit to secure payment should the customer not return the DVD after the first day. Hence, Redbox did not violate the Song-Beverly Act by requesting this personal data.
4. ***Behavioral Marketing and PII.*** The burgeoning practice of behavioral marketing, which is also sometimes termed "targeted marketing," involves examining the behavioral patterns of consumers to target advertisements to them. In this technique, companies generally do not track individuals through use of their names. Instead they utilize software to build personal profiles that exclude this item but that contain a wealth of details about the individual. Typically, these firms associate these personal profiles with a single alphanumerical code placed on an individual's computer. These codes are used to decide which advertisements people see as well as the kinds of products that are offered to them.

   While advertising networks may not know a person's name, identification of individuals is nonetheless possible in many cases. For example, enough

pieces of information linked to a single person, even in the absence of a name, Social Security number, or financial information, will permit identification of the individual. Nonetheless, online companies have attempted to short-circuit the discussion of privacy harms and necessary legal reforms by simply asserting that they do not collect PII.

5. ***Ohm on the PII Problem.*** In the view of Paul Ohm, privacy law must abandon its reliance on PII and find a new regulatory paradigm.[16] He argues that the concept of PII is unworkable and unfixable. He points to new re-identification research that has demonstrated that de-identified records can be re-identified "with astonishing ease." This occurs because there is already so much data available about individuals that is linked to their identity. To re-identify records, one can simply try to match the information in the records to other available data about an identified person. For example, Netflix, a popular online movie rental service, made a supposedly de-identified database of ratings publicly available as part of a contest to improve the predictive capabilities of its movie recommending software. Two researchers, Arvind Narayanan and Vitaly Shmatikov, found a way to link this data with the movie ratings that some participating individuals gave to films in the Internet Movie Database (IMDb), a popular website with information and ratings about movies.[17] They did this by matching the data to individuals' public movie ratings on IMDb.[18]

   Because data can be so readily linked to a person's identity, Ohm contends that the "list of potential PII will never stop growing until it includes everything." Ohm proposes that regulators abandon PII and instead "prevent privacy harm by squeezing and reducing the flow of information in society, even though in doing so they may need to sacrifice, at least a little, important counter values like innovation, free speech, and security." He would replace the current reliance on PII as a gatekeeper for privacy law with a cost-benefit analysis for *all* data processing and data collection of any kind. Ohm proposes that privacy regulation "should weigh the benefits of unfettered information flow against the cost of privacy harms." He proposes a minimum floor of safe handling of data for every data processor in the United States plus even stricter practices to be imposed on the entities that he terms "large entropy reducers." Ohm writes:

> Large entropy reducers are entities that amass massive databases containing so many links between so many disparate kinds of information that they represent a significant part of the database of ruin, even if they delete from their databases all particularly sensitive and directly linkable information. We can justify treating these entities differently using the language of duty and fault. Because large entropy reducers serve as one-stop shops for adversaries trying to link people to ruinous facts, they owe their data subjects a heightened duty of care. When a large entropy reducer loses control of its massive database, it causes much more harm than an entity holding much less data.

[16] Paul Ohm, *Broken Promises of Privacy*, 57 UCLA L. Rev. 1701 (2010).

[17] Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, 2008 IEEE Symp. on Security and Privacy 111 (Feb. 5, 2008), available at http://arxiv.org/PS_cache/cs/pdf/0610/0610105v2.pdf.

[18] Narayanan & Shmatikov concede that the results did not "imply anything about the percentage of IMDb users who can be identified in the Netflix Prize dataset." *Id.* For an insightful technical analysis of the limits of the Netflix study and how it is has been misunderstood, see Jane Yakowitz, *Tragedy of the Data Commons*, 25 Harv. J.L. & Tech. 1 (2011).

More specifically, Ohm identifies as "large entropy reducers" companies such as the credit reporting agencies (i.e., Equifax), data brokers (i.e., LexisNexis), and Internet search engines (i.e., Google). Do you think that a specific set of regulations should be devoted to companies such as the ones that Ohm identifies?

6. ***Schwartz and Solove Propose PII 2.0.*** In contrast to Ohm, Paul Schwartz and Daniel Solove contend that information privacy law needs a concept of PII.[19] Without such a concept, information privacy law will be a boundless area—it will grow to regulate all information use. At the same time, Schwartz and Solove also propose that PII must be reconceptualized if privacy law is to remain effective in the future.

   In their concept of PII 2.0, they propose three different regulatory categories, each of which would be treated differently. Schwartz and Solove write:

> Rather than a hard "on-off" switch, this approach allows legal safeguards for both identified and identifiable information, ones that permit tailored FIPs built around the different levels of risk to individuals. In our model of PII 2.0, information refers to (1) an identified, (2) identifiable, or (3) non-identifiable person. The continuum runs from actually being identified to no risk of identification, and our three categories divide up this spectrum and provide three different regimes of regulation. Because these categories do not have hard boundaries and are fluid, we define them in terms of standards.
>
> Information refers to an *identified* person when it singles out a specific individual from others. Put differently, a person has been identified when her identity is ascertained. There is general international agreement about the content of this category, albeit not of the implications of being placed in it. For example, in the U.S., the General Accounting Office, Office of Management and Budget, and National Institute of Standards and Technology associate this concept with information that distinguishes or traces a specific individual's identity.[20] In Europe, the Article 29 Group states that a person is identified "when, within a group of persons, he or she is 'distinguished' from all other members of the group."[21]
>
> In the middle of the risk continuum, information refers to an *identifiable* individual when a specific identification, while possible, is not a significantly probable event. In other words, an individual is identifiable when there is some non-remote possibility of future identification. The risk level is moderate to low. This information should be treated differently than an important sub-category of nominally identifiable information, where a linkage to a specific

[19] Paul Schwartz & Daniel Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1815 (2011).

[20] National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (PII) 2–1 (2010); General Accounting Office, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information* (May 2008); Office of Management & Budget, *Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (2007).

[21] Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data* 12 (June, 20, 2007).

> person has not yet been made, but where such a connection is more likely. . . . [S]uch nominally identifiable data should be treated the same as identified data.
>
> At the other end of the risk continuum, *non-identifiable* information carries only a remote risk of identification. Such data cannot be said to be relatable to a person taking account of the means reasonably likely to be used for identification. In certain kinds of data sets, for example, the original sample is so large that other information will not enable the identification of individuals.

Schwartz and Solove argue that re-identification is a risk rather than a certainty, and the law should be based upon the degree of risk. That risk, however, is changing, because the ability to transform non-PII into identified information depends in part on the amount of personal data about people that is available — the more data, the easier it is to find a match. The risk also depends upon technology, which is changing. How should privacy regulation deal with this evolving landscape? Does PII 2.0 adequately address this problem?

7. ***Risks in De-Identified Data?*** For Jane Yakowitz, the key question is "how much marginal risk does a public research database create in comparison to the background risks we already endure?"[22] Yakowitz assesses this marginal risk from data-sharing involving de-identified data as "trivially small." She reaches this conclusion by arguing that actual "adversaries" who will seek to de-identify are scarce, in part because of "lower hanging fruit," such as consumer databases that can be purchased, compared to anonymized databases. Yakowitz also points out that re-identifying subjects in anonymized databases is far from easy, but requires statistical expertise, and that "large repeat players" who share anonymized databases do not make "rookie mistakes."

   A white paper by Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada, and Khaled El Emam has argued along similar lines.[23] In their view, despite "a residual risk of re-identification, in the vast majority of cases, de-identification will protect the privacy of individuals, as long as additional safeguards are in place." In their four-step process, the re-identification risk exposure of a data disclosure depends upon: "the re-identification probability; the mitigating controls that are in place; the motives and capacity of the data recipient to re-identify the data; and the extent to which an inappropriate disclosure would be an invasion of privacy."

   Data security breach laws also rely on definitions of PII. We examine this area of law in the next chapter.

[22] Jane Yakowitz, *Tragedy of the Data Commons*, 25 Harv. J.L. & Tech.1 (2011).

[23] Ann Cavoukian & Khaled El Emam, *Dispelling the Myths Surrounding De-Identification: Anonymization Remains a Strong Tool for Protecting Privacy* (Information and Privacy Commissioner of Ontario, June 2011).

4. INJURY AND STANDING

An overarching issue in privacy cases is whether the privacy violation caused any harm. Suppose a company violates a promise made in its privacy policy not to share data with third parties. The company shares personal data about consumers with a marketing company that uses the data to create more tailored ad profiles and deliver targeted advertisements to consumers. Did the consumers suffer any harm?

Plaintiffs must typically allege a cognizable injury in order to have a viable cause of action. In federal courts, in order to have standing, the plaintiff

> must show that (1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. *Friends of the Earth, Inc. v. Laidlaw Envtl. Sys. (TOC), Inc.*, 528 U.S. 167 (2000).

If a plaintiff cannot establish standing, then a plaintiff's lawsuit cannot proceed forward in federal court.

Sometimes, statutes define the elements of a cognizable injury, but in the absence of such a statutorily defined harm, courts will look to general legal principles to determine if an injury occurred. In both data security breach cases and privacy cases, courts have struggled to recognize harm. Daniel Solove argues that courts often look for harms that are "visceral and vested":

> Harms must be *visceral* — they must involve some dimension of palpable physical injury or financial loss. And harms must be *vested* — they must have already occurred.
>
> For harms that involve emotional distress, courts are skeptical because people can too easily say they suffered emotional distress. It can be hard to prove or disprove statements that one suffered emotional distress, and these difficulties make courts very uneasy.
>
> For the future risk of harm, courts generally want to see harm that has actually manifested rather than harm that is incubating. Suppose you're exposed to a virus that silently waits in your bloodstream for 10 years and then suddenly might kill you. Most courts would send you away and tell you to come back after you've dropped dead, because then we would know for sure you're injured. But then, sadly, the statute of limitations will have run out, so it's too late to sue. Tough luck, the courts will say.[24]

Clapper v. Amnesty International USA, 133 S. Ct. (2013) has been a highly-influential standing case for lawsuits involving privacy and security violations. Although *Clapper* involved a constitutional challenge to national security surveillance, the case has had a significant impact on data breach and privacy litigation among private parties. In *Clapper*, a group of attorneys, journalists, and others contended that government surveillance under the Foreign Intelligence Surveillance Act (FISA) violated their constitutional rights. They could not prove that they were definitely under surveillance, but they had reason to fear they were

[24] Daniel J. Solove, *Privacy and Data Security Violations: What's the Harm*, LinkedIn (June 25, 2014), https://www.linkedin.com/today/post/article/20140625045136-2259773-privacy-and-data-security-violations-what-s-the-harm.

under surveillance because they represented or spoke to individuals whom the government would likely deem as suspicious.

The Supreme Court held that the plaintiffs could not establish standing. The Court reasoned that "it is speculative whether the Government will imminently target communications to which respondents are parties." The FISA "at most *authorizes*—but does not *mandate* or *direct*—the surveillance that respondents fear, respondents' allegations are necessarily conjectural. Simply put, respondents can only speculate as to how the Attorney General and the Director of National Intelligence will exercise their discretion in determining which communications to target."

The plaintiffs also contended that they were injured because they had to take measures to avoid the risk that they were under surveillance. "Respondents claim, for instance, that the threat of surveillance sometimes compels them to avoid certain e-mail and phone conversations, to 'tal[k] in generalities rather than specifics,' or to travel so that they can have in-person conversations." The Court rejected these costs as a basis for injury because "parties cannot manufacture standing by incurring costs in anticipation of non-imminent harm."

After *Clapper,* many federal courts have used the Supreme Court's decision to deny standing to plaintiffs in data breach cases when plaintiffs claim injury due to a risk of future harm or spending money on protective measures against such harm. There are, however, a number of courts that have distinguished *Clapper* and concluded that plaintiffs have alleged a concrete injury. See the chapter on data security for more about these cases.

SPOKEO, INC. V. ROBINS

136 S.Ct. 1540 (2016)

ALITO, J. This case presents the question whether respondent Robins has standing to maintain an action in federal court against petitioner Spokeo under the Fair Credit Reporting Act of 1970 (FCRA or Act).

Spokeo operates a "people search engine." If an individual visits Spokeo's Web site and inputs a person's name, a phone number, or an e-mail address, Spokeo conducts a computerized search in a wide variety of databases and provides information about the subject of the search. Spokeo performed such a search for information about Robins, and some of the information it gathered and then disseminated was incorrect. When Robins learned of these inaccuracies, he filed a complaint on his own behalf and on behalf of a class of similarly situated individuals.

The District Court dismissed Robins' complaint for lack of standing, but a panel of the Ninth Circuit reversed. . . .

The FCRA seeks to ensure "fair and accurate credit reporting." To achieve this end, the Act regulates the creation and the use of "consumer report[s]" by "consumer reporting agenc[ies]" for certain specified purposes, including credit transactions, insurance, licensing, consumer-initiated business transactions, and employment. Enacted long before the advent of the Internet, the FCRA applies to companies that regularly disseminate information bearing on an individual's

"credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living."

The Act . . . provides that "[a]ny person who willfully fails to comply with any requirement [of the Act] with respect to any [individual[3]] is liable to that [individual]" for, among other things, either "actual damages" or statutory damages of $100 to $1,000 per violation, costs of the action and attorney's fees, and possibly punitive damages. § 1681n(a).

Spokeo is alleged to qualify as a "consumer reporting agency" under the FCRA. It operates a Web site that allows users to search for information about other individuals by name, e-mail address, or phone number. In response to an inquiry submitted online, Spokeo searches a wide spectrum of databases and gathers and provides information such as the individual's address, phone number, marital status, approximate age, occupation, hobbies, finances, shopping habits, and musical preferences. According to Robins, Spokeo markets its services to a variety of users, including not only "employers who want to evaluate prospective employees," but also "those who want to investigate prospective romantic partners or seek other personal information." Persons wishing to perform a Spokeo search need not disclose their identities, and much information is available for free.

At some point in time, someone (Robins' complaint does not specify who) made a Spokeo search request for information about Robins, and Spokeo trawled its sources and generated a profile. By some means not detailed in Robins' complaint, he became aware of the contents of that profile and discovered that it contained inaccurate information. His profile, he asserts, states that he is married, has children, is in his 50's, has a job, is relatively affluent, and holds a graduate degree. According to Robins' complaint, all of this information is incorrect.

Robins filed a class-action complaint in the United States District Court for the Central District of California, claiming, among other things, that Spokeo willfully failed to comply with the FCRA requirements enumerated above. . . .

Although the Constitution does not fully explain what is meant by "[t]he judicial Power of the United States," it does specify that this power extends only to "Cases" and "Controversies," Art. III, § 2. . . .

Standing to sue is a doctrine rooted in the traditional understanding of a case or controversy. The doctrine developed in our case law to ensure that federal courts do not exceed their authority as it has been traditionally understood. The doctrine limits the category of litigants empowered to maintain a lawsuit in federal court to seek redress for a legal wrong.

Our cases have established that the "irreducible constitutional minimum" of standing consists of three elements. [Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992).] The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision. The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these elements. . . .

This case primarily concerns injury in fact, the "[f]irst and foremost" of standing's three elements. Injury in fact is a constitutional requirement, and "[i]t is settled that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing."

To establish injury in fact, a plaintiff must show that he or she suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." Lujan, 504 U.S., at 560.

Particularization is necessary to establish injury in fact, but it is not sufficient. An injury in fact must also be "concrete." Under the Ninth Circuit's analysis, however, that independent requirement was elided. As previously noted, the Ninth Circuit concluded that Robins' complaint alleges "concrete, de facto " injuries for essentially two reasons. First, the court noted that Robins "alleges that Spokeo violated his statutory rights, not just the statutory rights of other people." Second, the court wrote that "Robins's personal interests in the handling of his credit information are individualized rather than collective." Both of these observations concern particularization, not concreteness. We have made it clear time and time again that an injury in fact must be both concrete and particularized.

A "concrete" injury must be "de facto"; that is, it must actually exist. . . .

"Concrete" is not, however, necessarily synonymous with "tangible." Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.

In determining whether an intangible harm constitutes injury in fact, both history and the judgment of Congress play important roles. Because the doctrine of standing derives from the case-or-controversy requirement, and because that requirement in turn is grounded in historical practice, it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts. In addition, because Congress is well positioned to identify intangible harms that meet minimum Article III requirements, its judgment is also instructive and important. Thus, we said in Lujan that Congress may "elevat[e] to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law."

Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right. Article III standing requires a concrete injury even in the context of a statutory violation. For that reason, Robins could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III.

This does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness. *See,* e.g., Clapper v. Amnesty Int'l USA, 133 S.Ct. 1138 (2013). For example, the law has long permitted recovery by certain tort victims even if their harms may be difficult to prove or measure. Just as the common law permitted suit in such instances, the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in such a case need not allege any additional harm beyond the one Congress has identified.

In the context of this particular case, these general principles tell us two things: On the one hand, Congress plainly sought to curb the dissemination of false information by adopting procedures designed to decrease that risk. On the other hand, Robins cannot satisfy the demands of Article III by alleging a bare procedural violation. A violation of one of the FCRA's procedural requirements may result in no harm. For example, even if a consumer reporting agency fails to provide the required notice to a user of the agency's consumer information, that information regardless may be entirely accurate. In addition, not all inaccuracies cause harm or present any material risk of harm. An example that comes readily to mind is an incorrect zip code. It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm.

Because the Ninth Circuit failed to fully appreciate the distinction between concreteness and particularization, its standing analysis was incomplete. It did not address the question framed by our discussion, namely, whether the particular procedural violations alleged in this case entail a degree of risk sufficient to meet the concreteness requirement. We take no position as to whether the Ninth Circuit's ultimate conclusion—that Robins adequately alleged an injury in fact—was correct.

GINSBURG, J. joined by SOTOMAYOR, J. dissenting. . . . Judged by what we have said about "concreteness," Robins' allegations carry him across the threshold. . . .

Inspection of the Court's decisions suggests that the particularity requirement bars complaints raising generalized grievances, seeking relief that no more benefits the plaintiff than it does the public at large. Robins' claim does not present a question of that character. He seeks redress, not for harm to the citizenry, but for Spokeo's spread of misinformation specifically about him. . . .

Robins would not qualify, the Court observes, if he alleged a "bare" procedural violation, one that results in no harm, for example, "an incorrect zip code." Far from an incorrect zip code, Robins complains of misinformation about his education, family situation, and economic status, inaccurate representations that could affect his fortune in the job market. See Brief for Center for Democracy & Technology et al. as Amici Curiae (Spokeo's inaccuracies bore on Robins' "ability to find employment by creating the erroneous impression that he was overqualified for the work he was seeking, that he might be unwilling to relocate for a job due to family commitments, or that his salary demands would exceed what prospective employers were prepared to offer him."). The FCRA's procedural requirements aimed to prevent such harm. I therefore see no utility in returning this case to the Ninth Circuit to underscore what Robins' complaint already conveys concretely: Spokeo's misinformation "cause[s] actual harm to [his] employment prospects."

NOTES & QUESTIONS

1. ***How Tangible Must a "Concrete" Injury Be?*** Standing has been a particularly challenging issue in privacy cases, with many such cases being dismissed for lack of standing because of courts concluding that plaintiffs have not suffered harm. The Court states that a "concrete" injury "must actually exist" and must be "real and not abstract." Yet, the court also states that "we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete." Privacy is often an intangible injury. When is an intangible injury "real and not abstract"?

2. ***When Can Congress Define What Is Recognized as a Concrete Injury?*** The Court notes that Congress may "elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law." Congress can deem even injuries "previously inadequate in law" to be concrete injuries sufficient to confer standing.

   However, the Court also states:

   > Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right. Article III standing requires a concrete injury even in the context of a statutory violation. For that reason, Robins could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III.

   If legislatures are not limited to defining harms in the same way as courts, why should courts override a legislative determination of harm? In the FCRA, Congress determined that certain violations of the statute constituted a harm. Why does the Court not defer to Congress?

   What is the implication of *Spokeo* for statutory damages? Legislatures enact statutory damage provisions so that statutes may be enforced even if it is difficult to prove harm. Under *Spokeo*, people's rights under FCRA may be violated, Congress may have given people the right to sue to enforce these rights, but courts could still disallow people to sue. Is this a judicial usurpation of Congress's power as to how it wants its statutes to be enforced?

   What is a "bare procedural violation"? The Court states that "the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in such a case need not allege any *additional* harm beyond the one Congress has identified." Moreover, the Court states that a "real risk of harm" can "satisfy the requirement of concreteness." Additionally, the Court notes that "the law has long permitted recovery by certain tort victims even if their harms may be difficult to prove or measure." Taking these statements all together, what does the Court mean?

3. ***The Nature of the Harm.*** The Court notes: "[N]ot all inaccuracies cause harm or present any material risk of harm. An example that comes readily to mind is an incorrect zip code. It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm." Do you agree with this example? Is the dissent correct that Robins did allege a concrete injury?

IN RE GOOGLE, INC. PRIVACY POLICY LITIGATION

2013 WL 6248499 (N.D. Cal. 2013)

GREWAL, MAGISTRATE J. . . . By now, most people know who Google is and what Google does. Google serves billions of online users in this country and around the world. What started as simply a search engine has expanded to many

other products such as YouTube and Gmail. Google offers these products and most others without charge. With little or no revenue from its users, Google still manages to turn a healthy profit by selling advertisements within its products that rely in substantial part on users' personal identification information ("PII"). As some before have observed, in this model, the users are the real product.

Before March 1, 2012, Google maintained separate privacy policies for each of its products, each of which confirmed that Google used a user's PII to provide that particular product. These policies also confirmed that Google would not use the PII for any other purpose without the user's explicit consent. As Google put it, "[w]hen you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use." . . .

On March 1, 2012, Google announced a new policy. The majority of its separate privacy policies were eliminated in favor of a single, universal privacy policy that spells out that Google may combine a user's PII across multiple Google products. Google explained the basis for the change in policy as follows:

> Our new Privacy Policy makes clear that, if you're signed in, we may combine information that you've provided from one service with information from other services. In short, we'll treat you as a single user across all our products, which will mean simpler, more intuitive Google experience.

In other words, through the new policy, Google is explicit that it may combine PII collected from a user's Gmail or YouTube account, including the content of that account, with PII collected from that user's Google search queries, along with the user's activities on other Google products, such as Picasa, Maps, Docs, and Reader. This PII includes:

- first and last name;
- home or other physical address (including street name and city);
- current, physical location, a user's email address, and other online contact information (such as the identifier or screen name);
- IP address;
- telephone number (both home and mobile numbers);
- list of contacts;
- search history from Google's search engine;
- web surfing history from cookies placed on the computer; and
- posts on Google+.

Plaintiffs contend that Google's new policy violates its prior policies because the new policy no longer allows users to keep information gathered from one Google product separate from information gathered from other Google products. Plaintiffs further contend that Google's new policy violates users' privacy rights by allowing Google to take information from a user's Gmail account, for which users may have one expectation of privacy, for use in a different context, such as to personalize Google search engine results, or to personalize advertisements shown while a user is surfing the internet, products for which a user may have an entirely different expectation of privacy. In addition to commingling Plaintiffs' PII

across the various Google products, Plaintiff contend Google has shared Plaintiffs' PII with third-party entities who have partnered with Google in order to develop applications for the Google Play app store to help it place targeted advertisements.

. . .

To satisfy Article III, a plaintiff "must show that (1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." A suit brought by a plaintiff without Article III standing is not a "case or controversy," and an Article III court therefore lacks subject matter jurisdiction over the suit. In that event, the suit should be dismissed under Fed. R. Civ. Pro. 12(b)(1). The injury required by Article III may exist by virtue of "statutes creating legal rights, the invasion of which creates standing." In such cases, the "standing question . . . is whether the constitutional or standing provision on which the claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief." At all times the threshold question of standing "is distinct from the merits of [a] claim" and does not require "analysis of the merits." The Supreme Court also has instructed that the "standing inquiry requires careful judicial examination of a complaint's allegations to ascertain whether the particular plaintiff is entitled to an adjudication of the particular claims asserted."

A complaint must state a "short plain statement of the claim showing that the pleader is entitled to relief." While "detailed factual allegations" are not required, a complaint must include more than an unadorned, the defendant-unlawfully-harmed-me accusation." In other words, a complaint must have sufficient factual allegations to "state a claim to relief that is plausible on its face." A claim is facially plausible "when the pleaded factual content allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Accordingly, under Fed. R. Civ. P. 12(b)(6), which tests the legal sufficiency of the claims alleged in the complaint, "[d]ismissal can be based on the lack of cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory."

When evaluating a Rule 12(b)(6) motion, the court must accept all material allegations in the complaint as true and construe them in the light most favorable to the non-moving party. . . .

"Dismissal with prejudice and without leave to amend is not appropriate unless it is clear that the complaint could not be saved by amendment. A dismissal with prejudice, except one for lack of jurisdiction, improper venue, or failure to join a party operates as an adjudication on the merits. . . .

Before considering the standing question, however, the court cannot help but make a few observations. First, despite generating little or no discussion in most other cases, the issue of injury-in-fact has become standard fare in cases involving data privacy. In fact, the court is hard-pressed to find even one recent data privacy case, at least in this district, in which injury-in-fact has not been challenged. Second, in this district's recent case law on data privacy claims, injury-in-fact has proven to be a significant barrier to entry. And so even though injury-in-fact may not generally be Mount Everest, as then-Judge Alito observed, in data privacy cases in the Northern District of California, the doctrine might still reasonably be

described as Kilimanjaro. *Danvers Motor Co., Inc. v. Ford Motor Co.*, 432 F.3d 286, 294 (3d Cir. 2005).

1. *Personal Identification Information.* Plaintiffs claim that when Google combined information that Plaintiffs provided to discrete Google products, without Plaintiffs' consent, Google injured them in two different ways. First, Google did not compensate them for the substantial economic value of the combined information. Second, Google's unauthorized comingling of their information, especially their likeness, was a breach of contract. Neither alleged harm, however, is sufficient to establish an injury-in-fact.

. . . [I]njury-in-fact in this context requires more than an allegation that a defendant profited from a plaintiff's personal identification information. Rather, a plaintiff must allege how the defendant's use of the information deprived the plaintiff of the information's economic value. Put another way, a plaintiff must do more than point to the dollars in a defendant's pocket; he must sufficient allege that in the process he lost dollars of his own. Plaintiffs' allegations certainly plead that Google made money using information about them for which they were provided no compensation beyond free access to Google's services. But an allegation that Google profited is not enough equivalent to an allegation that such profiteering deprived Plaintiffs' of economic value from that same information.

As before, the court finds the reasoning in *LaCourt v. Specific Media,* [2011 WL 1661532, at *5 (C.D. Cal. 2011),] instructive. There the plaintiffs alleged that the defendant installed cookies to track users' internet browsing to build behavior profiles to better target advertisements. The court found the tracked users lacked standing because, among other reasons, they did not "explain how they were 'deprived' of the economic value of their personal information simply because their unspecified personal information was purportedly collected by a third party." Other courts have agreed.

Addressing a set of facts similar to the present case, in *In re Google Android User Privacy Litig.,* [No. 11–MD–02264 JSW, 2013 WL 1283236, at *4 (N.D. Cal. Mar. 26, 2013)] the court found no Article III standing where plaintiffs alleged that Google's unauthorized use of PII reduced its value to them because the plaintiffs failed to tie Google's use to their alleged loss, such as being foreclosed from capitalizing on its value. Here, Plaintiffs similarly have not alleged how Google's use of PII in any way deprives them of the ability to profit from the same information. . . .

Finally, although Plaintiffs assert that the breach of contract arising from Google's unauthorized commingling activities offers a separate basis for injury-in-fact, they still fail to articulate a sufficient contract injury. Nominal damages are not available in California for breach of contract, and the amended complaint does not allege any other injury based on the breach. In their opposition, Plaintiffs assert that "one of the most egregious ways in which Google breaches its contracts . . . is by misusing Plaintiffs' information to misappropriate their likeness. But even if this point in opposition were presented in the complaint itself, which it is not, Plaintiffs still cite no case law holding that a contract breach by itself constitutes an injury in fact. This is insufficient.

2. *Direct Economic Injuries.* The court next considers whether Plaintiffs have alleged direct economic injuries sufficient to establish injury-in-fact. As the Supreme Court has noted, "palpable economic injuries have long been recognized

as sufficient to lay the basis for standing." Plaintiffs each allege that they were injured when their Android devices sent their respective names, email addresses, and locations to the developer of each app they purchased or downloaded because they had to pay for the battery and bandwidth consumed by the unauthorized transmissions. Mr. Nisenbaum, representing the Android Device Switch Subclass, claims further injury in that he overpaid for his Android phone in 2010 because he would not have bought the phone had Google disclosed its intention to use his information as alleged in the complaint. Mr. Nisenbaum also claims that he replaced his Android phone with an iPhone in 2012 as a result of Google's policy change, causing him further economic injury.

The Court will consider each of these direct economic injury theories in turn to determine if they articulate "something more" than pure economic harm to support subject-matter jurisdiction under Rule 12(b)(1).

With respect to Plaintiffs' injury claims based on battery and bandwidth consumption, courts have found that the unauthorized use of system resources can suffice to establish a cognizable injury. For example, in *Goodman* [*vs. HTC*, No. C11–1793MJP, 2012 WL 2412070, at *5 (W.D. Wash. Jun. 26, 2012)], the court found standing based upon battery discharge where the application at issue sent fine location data every three hours or whenever the device's screen was refreshed. Similarly, in *In re iPhone Application Litigation* [844 F. Supp. 2d 1040, 1054–56 (N.D. Cal. 2012)], the court found standing where the device systematically collected and transmitted location information. In *In re Google Android User Privacy Litigation* [2013 WL 1283236, at *2, 4 (N.D. Cal. Mar. 26, 2013)], the plaintiffs did not clearly allege how frequently Google collected geolocation data from a phone, but did allege that collecting relocation data was particularly battery intensive, that "their batteries discharged more quickly[,] and that their services were interrupted." This latter allegation was deemed sufficient to establish standing. At the same time, in *Hernandez v. Path, Inc.* [2012 WL 5194120, at *8 (N.D. Cal. Oct. 19, 2012)], the court found that any harm from the use of phone resources in an app's uploading a user's address book a single time upon first running the app was *de minimis* and thus insufficient to establish injury.

Plaintiffs' allegations here are closer to *Goodman, iPhone I* and *Android* than *Hernandez.* Like *Hernandez,* Plaintiffs' alleged unauthorized battery consumption only happened infrequently, when a plaintiff first downloaded an app. But in *Hernandez* the allegedly unauthorized upload only happened once, when a plaintiff downloaded the Path app. Here, it happens each time a user downloads any app. The plaintiff who downloaded the most apps, according to the amended complaint, did so at least 27 times. In addition, like the plaintiffs in *Goodman* and *Android,* Plaintiffs here specifically allege a greater discharge of battery power as a result of unauthorized conduct and as in *iPhone I* the discharge is systemic rather than episodic. This is sufficient to establish more than a *de minimis* injury.

With respect to Mr. Nisenbaum's further allegations of injury, they, too, support standing for purposes of Article III.

First, the allegation that Mr. Nisenbaum bought a new phone after the policy change and that his motivation for choosing an iPhone over the Android device was substantially for privacy reasons, establishes that he was injured by making the purchase. To be sure, users frequently replace old phones for all kinds of reasons beyond privacy. For example, from the complaint, it appears Mr. Nisenbaum had his Android device for approximately two years, the length of most phone contracts that often include a discount for bundled phones, before purchasing a new phone. But Mr. Nisenbaum specifically alleges that but for the policy switch he would not have otherwise have bought a new phone. The alleged injury is fairly traceable to Google based on Mr. Nisenbaum's allegation that he relied on Google's previous policies in purchasing the Android phone in the first place.

Second, Mr. Nisembaum's allegations regarding overpayment establish injury. In *Pirozzi v. Apple* [913 F. Supp. 2d 840, 846–47 (N.D. Cal. 2012)], the court explained that Article III standing under an overpayment theory may be supported by "allegations [by plaintiffs] that, when they purchased their [ ] devices, they relied upon representations regarding privacy protection, which caused them to pay more than they would have for their devices." Similarly, in *Goodman,* the court found standing for overpayment of a smartphone where plaintiffs alleged they would have "paid less for the phones had [d]efendant's not misrepresented the relevant features." The court held that a "general averment of quality, alleged to be false, was sufficient to constitute an alleged injury in the form of overpayment." The allegations here are equally sufficient.

Google highlights that Mr. Nisenbaum has not alleged that he bought his phone from Google or that Google manufactured the phone. But the complaint is clear that Mr. Nisenbaum's phone ran on Android, Google's open-source operating system, and that in order to access the Google Play marketplace included in Android, Mr. Nisenbaum had to create a Google account. Under such circumstances, the alleged harm of overpayment to a third party is fairly traceable to Google. . . .

NOTES & QUESTIONS

1. ***Postscript.*** The *Google* court went on to analyze the various claims, and it found that none of the claims was viable, so the court granted Google's motion to dismiss. Note that in federal court, plaintiffs must establish sufficient injury for standing, and then must still establish sufficient facts to justify a prima facie case on various causes of action.
2. ***Financial Harm.*** Is the *Google* court looking for the appropriate type of harm? Recall that Warren and Brandeis defined privacy as primarily an emotional injury, not a financial one. Should courts be focusing on financial harm? Was there non-financial harm when Google changed its privacy policies? Should courts recognize such harm?

   In *In Re Google, Inc. Cookie Placement Consumer Privacy Litigation*, 988 F. Supp. 2d 434 (D. Del. 2013), plaintiffs alleged that Google "'tricked' their Apple Safari and/or Internet Explorer browsers into accepting cookies, which then allowed defendants to display targeted advertising." The court held that the plaintiffs couldn't prove a harm because they couldn't demonstrate that Google interfered with their ability to "monetize" their personal data:

   > Examining the facts alleged in the light most favorable to plaintiffs, the court concludes that, while plaintiffs have offered some evidence that the online personal information at issue has some modicum of identifiable value to an

individual plaintiff, plaintiffs have not sufficiently alleged that the ability to monetize their PII has been diminished or lost by virtue of Google's previous collection of it.

3. ***The EU Reaction.*** Google's consolidation of its privacy policies also led to a reaction in the European Union. On December 19, 2013, the Spanish Data Protection Authority fined it 900,000 Euros, or approximately $1.2 million, for violating Spanish data protection provisions. The *Agencia Española de Protección de Datos* (AEPD) found that the combination of data by the different Google services widely exceeded the reasonable expectations of the majority of users. It also noted that Google hindered and, in some cases, prevented rights of access, rectification, and cancellation. Finally, the AEPD declared that Google did not obtain valid consent from the concerned individuals.

   In France, the French Data Protection authority fined Google 150,000 Euros, or approximately $200,000, which was the maximum fine that French law permitted to be placed on first time violators. The *Commission nationale de l'information et des libertés* (CNIL) also required Google to publish a copy of its order on its website in France. The CNIL found that Google "did not sufficiently inform its users of the conditions in which their personal data are processed, nor of the purposes of this processing." Google also failed to comply with its obligation to obtain user consent and to define retention periods for the data that it processes. As a final matter, Google "permits itself to combine all the data it collects about its users across all its services without any legal basis."[25]

   What lessons do you draw from the different reactions in the EU and United States to this same action by Google?

4. ***Possible Future Harm and Mitigation Expenses.*** In privacy cases, plaintiffs have alleged that defendants' activities create risks of possible future harm. Courts have generally not been receptive to this argument. In *Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013), which we excerpted in Chapter 5, the U.S. Supreme Court held that plaintiffs failed to allege a legally cognizable injury when they challenged a provision of the law that permits the government to engage in surveillance of their communications. Although this case does not involve consumer privacy issues, its reasoning has applicability for consumer privacy cases.

   The plaintiffs claimed that there was an "objectively reasonable likelihood" that their communications would be monitored, and as a result, they had to take "costly and burdensome measures to protect the confidentiality of their international communications." The Supreme Court concluded that the plaintiffs were speculating and that "allegations of possible future injury are not sufficient" to establish an injury. According to the Court, "fears of hypothetical future harm" cannot justify the countermeasures the plaintiffs

[25] CNIL, *Deliberation No. 2013-420 of the Sanctions Committee of CNIL imposing a financial penalty against Google Inc.* (Jan. 3, 2014).

took. "Enterprising" litigants could establish an injury "simply by making an expenditure based on a nonparanoid fear."

In data breach cases, most courts have rejected claims that the breach increased the risk of future identity theft. *See, e.g., Amburgy v. Express Scripts, Inc.*, 671 F. Supp.2d 1046 (E.D. Mo. 2009); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006). Likewise, courts reject cases when plaintiffs spend money for mitigation expenses — measures to protect themselves against future harm. One case, however, accepted this theory. In *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011), the court held:

> Under Maine negligence law, damages must be both reasonably foreseeable, and, even if reasonably foreseeable, of the type which Maine has not barred for policy reasons. Generally, under Maine law, "the fundamental test [for both tort and contract recovery] is one of reasonable foreseeability: if the loss or injury for which damages are claimed was not reasonably foreseeable under the circumstances, there is no liability." But liability in negligence also "ordinarily requires proof of personal injury or property damage." . . . In cases of nonphysical harm, Maine courts limit recovery by considering not only reasonable foreseeability, but also relevant policy considerations such as "societal expectations regarding behavior and individual responsibility in allocating risks and costs." . . .
>
> It is clear that, as a matter of policy, Maine law "encourages plaintiffs to take reasonable steps to minimize losses caused by a defendant's negligence." To recover mitigation damages, plaintiffs need only show that the efforts to mitigate were reasonable, and that those efforts constitute a legal injury, such as actual money lost, rather than time or effort expended.
>
> Maine has interpreted this "reasonableness" requirement for mitigation, judging whether the decision to mitigate was reasonable "at the time it was made." . . .
>
> The Seventh Circuit, for example, has held that under Restatement § 919 incidental costs expended in good faith to mitigate harm are recoverable—even if the costs turn out to exceed the savings. . . .
>
> The Fourth Circuit has noted, applying Restatement § 919, that plaintiffs should not face "a Hobson's choice" between allowing further damage to occur or mitigating the damage at their own expense. Toll Bros., Inc. v. Dryvit Sys., Inc., 432 F.3d 564, 570 (4th Cir.2005) (applying Connecticut law). In Toll, a real estate developer removed and replaced defective stucco from homes that it built, and sued the stucco manufacturer in negligence to recover its costs. The court concluded that, as a matter of policy, a plaintiff may recover the cost of its reasonable attempts to mitigate, even if the injury is "wholly financial" in nature.

However, in the *Hannaford Brothers* case the information was obtained by a ring of identity thieves and some people were already victimized. The court noted that the plaintiffs "were not merely exposed to a hypothetical risk, but to a real risk of misuse." Another case that found standing in a data breach case is *Resnick v. AvMed Inc.* (11th Cir. 2012), which is excerpted in Chapter 10.

B. TORT LAW

DWYER V. AMERICAN EXPRESS CO.

652 N.E.2d 1351 (Ill. App. 1995)

BUCKLEY, J. Plaintiffs, American Express cardholders, appeal the circuit court's dismissal of their claims for invasion of privacy and consumer fraud against defendants, American Express Company, American Express Credit Corporation, and American Express Travel Related Services Company, for their practice of renting information regarding cardholder spending habits.

On May 13, 1992, the New York Attorney General released a press statement describing an agreement it had entered into with defendants. The following day, newspapers reported defendants' actions which gave rise to this agreement. According to the news articles, defendants categorize and rank their cardholders into six tiers based on spending habits and then rent this information to participating merchants as part of a targeted joint-marketing and sales program. For example, a cardholder may be characterized as "Rodeo Drive Chic" or "Value Oriented." In order to characterize its cardholders, defendants analyze where they shop and how much they spend, and also consider behavioral characteristics and spending histories. Defendants then offer to create a list of cardholders who would most likely shop in a particular store and rent that list to the merchant.

Defendants also offer to create lists which target cardholders who purchase specific types of items, such as fine jewelry. The merchants using the defendants' service can also target shoppers in categories such as mail-order apparel buyers, home-improvement shoppers, electronics shoppers, luxury lodgers, card members with children, skiers, frequent business travelers, resort users, Asian/European travelers, luxury European car owners, or recent movers. Finally, defendants offer joint-marketing ventures to merchants who generate substantial sales through the American Express card. Defendants mail special promotions devised by the merchants to its cardholders and share the profits generated by these advertisements. . . .

Plaintiffs have alleged that defendants' practices constitute an invasion of their privacy [in particular, a violation of the intrusion upon seclusion tort]. . . .

. . . [There are] four elements [to intrusion upon seclusion] which must be alleged in order to state a cause of action: (1) an unauthorized intrusion or prying into the plaintiff's seclusion; (2) an intrusion which is offensive or objectionable to a reasonable man; (3) the matter upon which the intrusion occurs is private; and (4) the intrusion causes anguish and suffering. . . .

Plaintiffs' allegations fail to satisfy the first element, an unauthorized intrusion or prying into the plaintiffs' seclusion. The alleged wrongful actions involve the defendants' practice of renting lists that they have compiled from information contained in their own records. By using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences. . . .

Plaintiffs claim that because defendants rented lists based on this compiled information, this case involves the disclosure of private financial information and most closely resembles cases involving intrusion into private financial dealings, such as bank account transactions. Plaintiffs cite several cases in which courts have recognized the right to privacy surrounding financial transactions.

However, we find that this case more closely resembles the sale of magazine subscription lists, which was at issue in *Shibley v. Time, Inc.* In *Shibley*, the plaintiffs claimed that the defendant's practice of selling and renting magazine subscription lists without the subscribers' prior consent "constitut[ed] an invasion of privacy because it amount[ed] to a sale of individual 'personality profiles,' which subjects the subscribers to solicitations from direct mail advertisers." The plaintiffs also claimed that the lists amounted to a tortious appropriation of their names and "personality profiles." . . .

The *Shibley* court found that an Ohio statute, which permitted the sale of names and addresses of registrants of motor vehicles, indicated that the defendant's activity was not an invasion of privacy. . . .

Defendants rent names and addresses after they create a list of cardholders who have certain shopping tendencies; they are not disclosing financial information about particular cardholders. These lists are being used solely for the purpose of determining what type of advertising should be sent to whom. We also note that the Illinois Vehicle Code authorizes the Secretary of State to sell lists of names and addresses of licensed drivers and registered motor-vehicle owners. Thus, we hold that the alleged actions here do not constitute an unreasonable intrusion into the seclusion of another. We so hold without expressing a view as to the appellate court conflict regarding the recognition of this cause of action.

Considering plaintiffs' appropriation claim, the elements of the tort are: an appropriation, without consent, of one's name or likeness for another's use or benefit. This branch of the privacy doctrine is designed to protect a person from having his name or image used for commercial purposes without consent. According to the Restatement, the purpose of this tort is to protect the "interest of the individual in the exclusive use of his own identity, in so far as it is represented by his name or likeness." Illustrations of this tort provided by the Restatement include the publication of a person's photograph without consent in an advertisement; operating a corporation named after a prominent public figure without the person's consent; impersonating a man to obtain information regarding the affairs of the man's wife; and filing a lawsuit in the name of another without the other's consent.

Plaintiffs claim that defendants appropriate information about cardholders' personalities, including their names and perceived lifestyles, without their consent. Defendants argue that their practice does not adversely affect the interest of a cardholder in the "exclusive use of his own identity," using the language of the Restatement. Defendants also argue that the cardholders' names lack value and that the lists that defendants create are valuable because "they identify a useful aggregate of potential customers to whom offers may be sent.". . .

To counter defendants' argument, plaintiffs point out that the tort of appropriation is not limited to strictly commercial situations.

Nonetheless, we again follow the reasoning in *Shibley* and find that plaintiffs have not stated a claim for tortious appropriation because they have failed to allege the first element. Undeniably, each cardholder's name is valuable to defendants. The more names included on a list, the more that list will be worth. However, a

single, random cardholder's name has little or no intrinsic value to defendants (or a merchant). Rather, an individual name has value only when it is associated with one of defendants' lists. Defendants create value by categorizing and aggregating these names. Furthermore, defendants' practices do not deprive any of the cardholders of any value their individual names may possess. . . .

NOTES & QUESTIONS

1. **Shibley v. Time.** In *Shibley v. Time, Inc.,* 341 N.E.2d 337 (Ohio Ct. App. 1975), the plaintiff sued the publishers of a number of magazines for selling subscription lists to direct mail advertising businesses. The plaintiff sued under the public disclosure tort and the appropriation tort. Despite the fact that the purchasers of the lists can learn about the plaintiff's lifestyle from the data, the court dismissed the plaintiff's public disclosure action. The court found that the sale of the lists did not "cause mental suffering, shame or humiliation to a person of ordinary sensibilities." The court also rejected the plaintiff's argument that by selling the lists, the defendants were appropriating his name and likeness because the tort of appropriation is available only in those "situations where the plaintiff's name or likeness is displayed to the public to indicate that the plaintiff indorses the defendant's product or business."

   According to *Shibley* and *Dwyer*, why does the public disclosure tort fail to provide a remedy for the disclosure of personal information to other companies? Why does the tort of intrusion upon seclusion fail? Why does the tort of appropriation fail? More generally, can tort law adequately remedy the privacy problems created by profiling and databases?[26]

2. ***A Fair Information Practices Tort?*** Sarah Ludington recommends that a new tort should be developed in the common law, one that "would impose on data traders a duty to use Fair Information Practices (based on the principles of notice, choice, access, and security)." Why the common law rather than legislation? Ludington argues:

   > [B]ecause it is now clear that industry lobbying has succeeded while self-regulation has failed, and that legislatures have either failed to act or provided solutions that inadequately address the injuries, individuals must — indeed, should — look to the judiciary to help resolve the misuse of personal information.[27]

   Would the use of the common law to regulate the collection and use of personal data be effective or appropriate? What would be the strengths and weaknesses of such a regulatory approach?

[26] For an interesting argument about how the tort of breach of confidentiality might provide a weak but potential solution to the problem, see Jessica Litman, *Information Privacy/Information Property*, 52 Stan. L. Rev. 1283 (2000). For a discussion of the use of the tort of appropriation, see Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling,* 98 Nw. U. L. Rev. 63 (2003).

[27] Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 Md. L. Rev. 140, 172-73 (2007).

3. ***Defining the Harm.*** What is the harm of commercial entities collecting and using personal information? One might contend that the kind of information that companies collect about individuals is not very sensitive or intimate. How much is a person harmed by sharing data that she prefers Coke to Pepsi or Puffs to Kleenex? Is there a significant privacy problem in revealing that a person has purchased tennis products, designer sunglasses, orange juice, or other things? One might view the harm as so minimal as to be trivial.

   Does information about a person's consumption patterns reveal something about that person's identity? Stan Karas argues that "consumption patterns may identify one as a liberal, moderate Republican, radical feminist or born-again Christian. . . . For some individuals, consumption is no longer a way of expressing identity but is synonymous with identity. . . . [T]he identity of many subcultures is directly related to distinctive patterns of consumption. One need only think of the personal styles of punk rockers, hip-hoppers, or Harley-fetishizing bikers."[28]

   According to Jerry Kang, data collection and compiling is a form of surveillance that inhibits individual freedom and choice: "[I]information collection in cyberspace is more like surveillance than like casual observation." He notes that "surveillance leads to self-censorship. This is true even when the observable information would not be otherwise misused or disclosed."[29]

   Daniel Solove contends that the problem of computer databases does not stem from surveillance. He argues that numerous theorists describe the problem in terms of the metaphor of Big Brother, the ruthless totalitarian government in George Orwell's *1984*, which constantly monitors its citizens. Solove contends that the Big Brother metaphor fails to adequately conceptualize the problem:

   > A large portion of our personal information involves facts that we are not embarrassed about: our financial information, race, marital status, hobbies, occupation, and the like. Most people surf the web without wandering into its dark corners. The vast majority of the information collected about us concerns relatively innocuous details. The surveillance model does not explain why the recording of this non-taboo information poses a problem.[30]

   In contrast, Solove proposes that data collection and processing is most aptly captured by Franz Kafka's *The Trial*, where the protagonist (Joseph K.) is arrested by officials from a clandestine court system but is not informed of the reason for his arrest. From what little he manages to learn about the court system, which operates largely in secret, Joseph K. discovers that a vast bureaucratic court has examined his life and assembled a dossier on him. His records, however, are "inaccessible," and K.'s life gradually becomes taken over by his frustrating quest for answers:

   > *The Trial* captures the sense of helplessness, frustration, and vulnerability one experiences when a large bureaucratic organization has control over a vast dossier of details about one's life. At any time, something could happen to

[28] Stan Karas, *Privacy, Identity, Databases,* 52 Am. U. L. Rev. 393, 438-39 (2002).

[29] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193 (1998).

[30] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393 (2001).

> Joseph K.; decisions are made based on his data, and Joseph K. has no say, no knowledge, and no ability to fight back. He is completely at the mercy of the bureaucratic process. . . .
>
> The problem with databases emerges from subjecting personal information to the bureaucratic process with little intelligent control or limitation, resulting in a lack of meaningful participation in decisions about our information. . . .
>
> Under this view, the problem with databases and the practices currently associated with them is that they disempower people. They make people vulnerable by stripping them of control over their personal information. There is no diabolical motive or secret plan for domination; rather, there is a web of thoughtless decisions made by low-level bureaucrats, standardized policies, rigid routines, and a way of relating to individuals and their information that often becomes indifferent to their welfare.[31]

Joel Reidenberg points out that the lack of protection of information privacy will "destroy anonymity" and take away people's "freedom to choose the terms of personal information disclosure."[32] According to Paul Schwartz, the lack of privacy protection can threaten to expose not just information about what people purchase, but also information about their communication and consumption of ideas:

> In the absence of strong rules for information privacy, Americans will hesitate to engage in cyberspace activities—including those that are most likely to promote democratic self-rule. . . . Current polls already indicate an aversion on the part of some people to engage even in basic commercial activities on the Internet. Yet, deliberative democracy requires more than shoppers; it demands speakers and listeners. But who will speak or listen when this behavior leaves finely-grained data trails in a fashion that is difficult to understand or anticipate?[33]

4. ***Using Consumers in Ads: Facebook's Sponsored Stories.*** In *Fraley v. Facebook*, 830 F. Supp. 2d 785 (N.D. Cal. 2011), plaintiffs sued Facebook for its "Sponsored Stories" advertising program. A Sponsored Story is a paid ad appearing on a person's Facebook page. It uses the name and photo of a person's friend who "likes" the advertiser:

> For example, Plaintiff Angel Fraley, who registered as a member with the name Angel Frolicker, alleges that she visited Rosetta Stone's Facebook profile page and clicked the "Like" button in order to access a free software demonstration. Subsequently, her Facebook user name and profile picture, which bears her likeness, appeared on her Friends' Facebook pages in a "Sponsored Story" advertisement consisting of the Rosetta Stone logo and the sentence, "Angel Frolicker likes Rosetta Stone."

Among the causes of action plaintiffs brought was appropriation of name or likeness under Cal. Civ. Code § 3344. Facebook moved to dismiss. Facebook

---

[31] *Id.*

[32] Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 Iowa L. Rev. 497 (1995).

[33] Paul M. Schwartz, *Privacy and Democracy in Cyberspace,* 52 Vand. L. Rev. 1609, 1651 (1999).

argued that the plaintiffs consented to being used in the ads because it had stated in its Terms of Use:

> You can use your privacy settings to limit how your name and profile picture may be associated with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. You give us permission to use your name and [Facebook] profile picture in connection with that content, subject to the limits you place.

The plaintiffs argued that Sponsored Stories did not exist when they signed up with Facebook and were never informed before they were suddenly used in the ads. The court held that there were factual issues in dispute on the consent issue that prevented dismissal.

Facebook also argued that there was no injury. The court however, concluded that plaintiffs had alleged sufficient facts to establish injury to withstand a motion to dismiss:

> Here, Plaintiffs allege not that they suffered mental anguish as a result of Defendant's actions, but rather that they suffered economic injury because they were not compensated for Facebook's commercial use of their names and likenesses in targeted advertisements to their Facebook Friends. Defendant does not deny that Plaintiffs may assert economic injury, but insists that, because they are not celebrities, they must demonstrate some preexisting commercial value to their names and likenesses, such as allegations that they "previously received remuneration for the use of their name or likeness, or that they have ever sought to obtain such remuneration."
>
> First, the Court finds nothing in the text of the statute or in case law that supports Defendant's interpretation of § 3344 as requiring a plaintiff pleading economic injury to provide proof of *preexisting* commercial value and efforts to capitalize on such value in order to survive a motion to dismiss. The plain text of § 3344 provides simply that "[a]ny person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner . . . for purposes of advertising or selling . . . without such person's consent . . . shall be liable for any damages sustained by the person or persons injured as a result thereof." The statutory text makes no mention of preexisting value, and in fact can be read to presume that a person whose name, photograph, or likeness is used by another for commercial purposes without their consent is "injured as a result thereof."
>
> Nor does the Court find any reason to impose a higher pleading standard on non-celebrities than on celebrities. California courts have clearly held that "the statutory right of publicity exists for celebrity and non-celebrity plaintiffs alike."
>
> Moreover, . . . the Court finds that Plaintiffs' allegations satisfy the requirements for pleading a claim of economic injury under § 3344. Plaintiffs quote Facebook CEO Mark Zuckerberg stating that "[n]othing influences people more than a recommendation from a trusted friend. A trusted referral influences people more than the best broadcast message. A trusted referral is the Holy Grail of advertising." . . .

In August 2013, the court in this case approved a $20 million settlement with Facebook. As this casebook goes to press, there is an appeal to the settlement

that argues that it violates state law in allowing Facebook to use images of minors without parental consent.[34]

REMSBURG V. DOCUSEARCH, INC.

816 A.2d 1001 (N.H. 2003)

DALIANIS, J. . . . [Liam Youens contacted Docusearch and purchased the birth date of Amy Lynn Boyer for a fee. He again contacted Docusearch and placed an order for Boyer's SSN. Docusearch obtained Boyer's SSN from a credit reporting agency and provided it to Youens. Youens then asked for Boyer's employment address. Docusearch hired a subcontractor, Michele Gambino, who obtained it by making a "pretext" phone call to Boyer. Gambino lied about her identity and the purpose of the call, and she obtained the address from Boyer. The address was then given to Youens. Shortly thereafter, Youens went to Boyer's workplace and shot and killed her and then killed himself.]

All persons have a duty to exercise reasonable care not to subject others to an unreasonable risk of harm. Whether a defendant's conduct creates a risk of harm to others sufficiently foreseeable to charge the defendant with a duty to avoid such conduct is a question of law, because "the existence of a duty does not arise solely from the relationship between the parties, but also from the need for protection against reasonably foreseeable harm." Thus, in some cases, a party's actions give rise to a duty. Parties owe a duty to those third parties foreseeably endangered by their conduct with respect to those risks whose likelihood and magnitude make the conduct unreasonably dangerous.

In situations in which the harm is caused by criminal misconduct, however, determining whether a duty exists is complicated by the competing rule "that a private citizen has no general duty to protect others from the criminal attacks of third parties." This rule is grounded in the fundamental unfairness of holding private citizens responsible for the unanticipated criminal acts of third parties, because "[u]nder all ordinary and normal circumstances, in the absence of any reason to expect the contrary, the actor may reasonably proceed upon the assumption that others will obey the law."

In certain limited circumstances, however, we have recognized that there are exceptions to the general rule where a duty to exercise reasonable care will arise. We have held that such a duty may arise because: (1) a special relationship exists; (2) special circumstances exist; or (3) the duty has been voluntarily assumed. The special circumstances exception includes situations where there is "an especial temptation and opportunity for criminal misconduct brought about by the defendant." This exception follows from the rule that a party who realizes or should realize that his conduct has created a condition which involves an unreasonable risk of harm to another has a duty to exercise reasonable care to prevent the risk from occurring. The exact occurrence or precise injuries need not have been foreseeable. Rather, where the defendant's conduct has created an

[34] For more on the case and a proposed "holistic economic and non-economic approach to the right of publicity" in online social networks, see Jesse Koehler, Fraley v. Facebook: *The Right of Publicity in Online Social Networks*, 28 Berkeley Tech. L.J. 963 (2013).

unreasonable risk of criminal misconduct, a duty is owed to those foreseeably endangered.

Thus, if a private investigator or information broker's (hereinafter "investigator" collectively) disclosure of information to a client creates a foreseeable risk of criminal misconduct against the third person whose information was disclosed, the investigator owes a duty to exercise reasonable care not to subject the third person to an unreasonable risk of harm. In determining whether the risk of criminal misconduct is foreseeable to an investigator, we examine two risks of information disclosure implicated by this case: stalking and identity theft.

It is undisputed that stalkers, in seeking to locate and track a victim, sometimes use an investigator to obtain personal information about the victims.

Public concern about stalking has compelled all fifty States to pass some form of legislation criminalizing stalking. Approximately one million women and 371,000 men are stalked annually in the United States. Stalking is a crime that causes serious psychological harm to the victims, and often results in the victim experiencing post-traumatic stress disorder, anxiety, sleeplessness, and sometimes, suicidal ideations.

Identity theft, *i.e.*, the use of one person's identity by another, is an increasingly common risk associated with the disclosure of personal information, such as a SSN. A person's SSN has attained the status of a quasi-universal personal identification number. At the same time, however, a person's privacy interest in his or her SSN is recognized by state and federal statutes. . . .

Like the consequences of stalking, the consequences of identity theft can be severe. . . . Victims of identity theft risk the destruction of their good credit histories. This often destroys a victim's ability to obtain credit from any source and may, in some cases, render the victim unemployable or even cause the victim to be incarcerated.

The threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client. And we so hold. This is especially true when, as in this case, the investigator does not know the client or the client's purpose in seeking the information. . . .

[The plaintiff also brought an action for intrusion upon seclusion.] A tort action based upon an intrusion upon seclusion must relate to something secret, secluded or private pertaining to the plaintiff. Moreover, liability exists only if the defendant's conduct was such that the defendant should have realized that it would be offensive to persons of ordinary sensibilities.

In addressing whether a person's SSN is something secret, secluded or private, we must determine whether a person has a reasonable expectation of privacy in the number. . . . As noted above, a person's interest in maintaining the privacy of his or her SSN has been recognized by numerous federal and state statutes. As a result, the entities to which this information is disclosed and their employees are bound by legal, and, perhaps, contractual constraints to hold SSNs in confidence to ensure that they remain private. Thus, while a SSN must be disclosed in certain circumstances, a person may reasonably expect that the number will remain private.

Whether the intrusion would be offensive to persons of ordinary sensibilities is ordinarily a question for the fact-finder and only becomes a question of law if reasonable persons can draw only one conclusion from the evidence. The evidence underlying the certified question is insufficient to draw any such conclusion here, and we therefore must leave this question to the fact-finder. In making this determination, the fact-finder should consider "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded." Accordingly, a person whose SSN is obtained by an investigator from a credit reporting agency without the person's knowledge or permission may have a cause of action for intrusion upon seclusion for damages caused by the sale of the SSN, but must prove that the intrusion was such that it would have been offensive to a person of ordinary sensibilities.

We next address whether a person has a cause of action for intrusion upon seclusion where an investigator obtains the person's work address by using a pretextual phone call. We must first establish whether a work address is something secret, secluded or private about the plaintiff.

In most cases, a person works in a public place. "On the public street, or in any other public place, [a person] has no legal right to be alone." . . . Thus, where a person's work address is readily observable by members of the public, the address cannot be private and no intrusion upon seclusion action can be maintained.

[Additionally, the plaintiff brought a cause of action for appropriation.] "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." *Restatement (Second) of Torts* § 652E.

. . . Appropriation is not actionable if the person's name or likeness is published for "purposes other than taking advantage of [the person's] reputation, prestige or other value" associated with the person. Thus, appropriation occurs most often when the person's name or likeness is used to advertise the defendant's product or when the defendant impersonates the person for gain.

An investigator who sells personal information sells the information for the value of the information itself, not to take advantage of the person's reputation or prestige. The investigator does not capitalize upon the goodwill value associated with the information but rather upon the client's willingness to pay for the information. In other words, the benefit derived from the sale in no way relates to the social or commercial standing of the person whose information is sold. Thus, a person whose personal information is sold does not have a cause of action for appropriation against the investigator who sold the information. . . .

NOTES & QUESTIONS

1. ***The Scope of the Duty.*** The court concludes that Docusearch has a duty to people "foreseeably endangered" by its disclosure of personal information. Is this too broad a duty to impose on those who collect and disseminate personal data? What could Docusearch have done to avoid being negligent in this case? Suppose Jill tells Jack the address of Roe. Jack goes to Roe's house and kills her. Based on *Remsburg*, can Jill be liable?

2. ***Tort Liability and the First Amendment.*** Does liability for Docusearch implicate the First Amendment?

C. CONTRACT LAW

1. PRIVACY POLICIES

Privacy policies are statements made by companies about their practices regarding personal information. Privacy policies are also referred to as "privacy notices." Increasingly, companies on the Internet are posting privacy policies, and statutes such as the Gramm-Leach-Bliley Act require certain types of companies (financial institutions, insurance companies, and brokerage companies) to maintain privacy policies.

One of the common provisions of many privacy policies is an "opt-out" provision. An opt-out provision establishes a default rule that the company can use or disclose personal information in the ways it desires so long as the consumer does not indicate otherwise. The consumer must take affirmative steps, such as checking a box, calling the company, or writing a letter, to express her desire to opt out of a particular information use or disclosure. In contrast, an "opt-in" provision establishes a default rule that the company cannot use or disclose personal information without first obtaining the express consent of the individual.

JEFF SOVERN, *OPTING IN, OPTING OUT, OR NO OPTIONS AT ALL: THE FIGHT FOR CONTROL OF PERSONAL INFORMATION*

74 Wash. L. Rev. 1033 (1999)

. . . [F]ew consumers understand how much of their personal information is for sale, although they may have a general idea that there is a trade in personal data and that the specifics about that trade are kept from them. . . .

. . . [C]onsumers cannot protect their personal information when they are unaware of how it is being used by others. . . .

The second reason consumers have not acted to protect their privacy, notwithstanding surveys that suggest considerable consumer concern with confidentiality, has to do with how difficult it is to opt out. . . .

. . . Even if consumers can obtain the information needed to opt out, the cost in time and money of communicating and negotiating with all the relevant information gatherers may be substantial. . . .

Companies may not be eager to offer opt-outs because they may rationally conclude that they will incur costs when consumers opt out, while receiving few offsetting benefits. When consumers exercise the option of having their names deleted, mailing lists shrink and presumably become less valuable. . . .

Because of these added costs, companies might decide that while they must offer an opt-out plan, they do not want consumers to take advantage of it. . . . [C]ompanies that offer opt-outs have an incentive to increase the transaction costs incurred by consumers who opt out. . . .

Companies can increase consumers' transaction costs in opting out in a number of ways. A brochure titled "Privacy Notice," which my local cable company included with its bill, provides an example. This Privacy Notice discussed, among other things, how cable subscribers could write to the company to ask that the company not sell their names and other information to third parties. There are at least four reasons why this particular notice may not be effective in eliciting a response from consumers troubled by the sale of their names to others.

First, the Privacy Notice may be obscured by other information included in the mailing. . . .

The second reason why consumers may not respond to the Privacy Notice is its length. The brochure is four pages long and contains 17 paragraphs, 36 sentences, and 1062 words. . . .

Some companies have gone in the other direction, providing so little information in such vague terms that consumers are unable to discern what they are being told. . . .

A third reason why the Privacy Notice may not be effective stems from its prose. Notwithstanding the Plain Language Law in my home state, computer analysis of the text found it extremely difficult, requiring more than a college education for comprehension. By comparison, a similar analysis of this Article found that it required a lower reading level than that of the Privacy Notice.

[Sovern suggests that an opt-in system would be more preferable than an opt-out system.]

One benefit of an opt-in system is that it minimizes transaction costs. While some transaction costs are inevitable in any system in which consumers can opt out or opt in, strategic-behavior transaction costs, at least, can be avoided by using a system which discourages parties from generating such costs. The current system encourages businesses to inflate strategic-behavior costs to increase their own gains, albeit at the expense of consumers and the total surplus from exchange. An opt-in system would encourage businesses to reduce strategic-behavior costs without giving consumers an incentive to increase these costs. Instead of an opt-out situation in which merchants are obligated to provide a message they do not wish consumers to receive, an opt-in regime would harness merchants' efforts in providing a message they want the consumer to receive. . . .

An opt-in system thus increases the likelihood that consumers will choose according to their preferences rather than choosing according to the default. . . .

MICHAEL E. STATEN & FRED H. CATE, *THE IMPACT OF OPT-IN PRIVACY RULES ON RETAIL MARKETS: A CASE STUDY OF MBNA*

52 Duke L.J. 745, 750-51, 766, 770-74, 776 (2003)

To illustrate the costs of moving to an opt-in system, we examine MBNA Corporation, a financial institution that offers consumers a variety of loan and insurance products (primarily credit cards), takes deposits, but operates entirely without a branch network. Incorporated in 1981 and publicly traded since 1991, the company has compiled a stunning growth record in just two decades. As of the end of 2000, the company provided credit cards and other loan products to 51 million consumers, had $89 billion of loans outstanding, and serviced 15 percent of all Visa/MasterCard credit card balances outstanding in the United States.

MBNA's ability to access and use information about potential and existing customers is largely responsible for it becoming the second largest credit card issuer in the United States in less than twenty years. . . . MBNA harnessed information technology as the engine for establishing and building customer relationships without ever physically meeting its customers. By using direct mail, telephone and, most recently, Internet contacts, the company has reached out to new prospects throughout the population, regardless of where they live, with offers tailored to their individual interests. . . .

At the core of its marketing and targeting strategies is the proposition that consumers who share a common institutional bond or experience will have an affinity for using a card that lets them demonstrate their affiliation each time they use it to pay for a purchase. . . . Following this "affinity group" marketing strategy, MBNA designs a card product tailored to members of a particular group, negotiates a financial arrangement with the organization for the exclusive rights to market an affinity card to its members, and uses the member list as a source of potential names to contact via direct mail or telemarketing. . . .

Given that MBNA's fundamental business is lending money via an unsecured credit card with a revolving line of credit attached, the company wants to put the card in the hands of customers who will use it, but who will not default on their balances. Consequently, MBNA uses information to screen prospects both before it makes card offers (the targeting process) and after it receives applications (the underwriting process). . . .

How large a drag does an "explicit-consent" system impose on economic efficiency? According to the U.S. Postal Service, 52 percent of unsolicited mail in this country is never read. If that figure translates to opt-in requests, then more than half of all consumers in an opt-in system would lose the benefits or services that could result from the use of personal information because the mandatory request for consent would never receive their attention. Moreover, even if an unsolicited offer is read, experience with company-specific and industry-wide opt-out lists demonstrates that less than 10 percent of the U.S. population ever opts out of a mailing list — often the figure is less than 3 percent. Indeed, the difficulty (and cost) of obtaining a response of any sort from consumers is the primary drawback of an opt-in approach. . . .

MBNA's core product is the affinity card tailored for and marketed to each of more than 4,700 affinity groups. . . . [T]he foundation of MBNA's affinity strategy is access to the member lists of each of its affinity organizations. . . . [A] third-party opt-in regime could effectively end MBNA's unique direct marketing approach by sharply limiting an organization's ability to share its member list. . . .

Like all major credit card issuers, MBNA uses personal information to increase the chance that its credit card offer will reach an interested and qualified customer. This process greatly reduces the number of solicitations that must be sent to achieve a given target volume of new accounts, thereby reducing the cost of account acquisition. It also reduces the volume of junk mail in the form of card offers sent to consumers who are not qualified. Third-party or affiliate opt-in systems would eliminate MBNA's access to a significant portion of the information that it currently uses to identify which individuals on the member lists

it receives would be good prospects for a given credit card or other product. A blanket opt-in system applicable to marketing activities would impose similar limits. . . .

NOTES & QUESTIONS

1. ***Opt Out vs. Opt In.*** Do you agree with Sovern that an opt-in policy is more efficient than an opt-out policy? Do you think that an opt-in policy is feasible? Are the views of Staten and Cate convincing on this score? Do you think opt out or opt in should be required by law?
2. ***Internalizing Costs.*** Staten and Cate claim that MBNA's business model will be threatened by opt in. This business model relies in part, however, on sending out 400 million of mostly unwanted solicitations for credit in order to receive a 0.6 percent response rate. In other words, this model views as an externality the added cost of sorting through mail for 99.4 percent of those individuals solicited. Should MBNA be obliged to internalize these costs?
3. ***Does Privacy-Self Management Work?*** Privacy policies form the backbone of what Daniel Solove calls "privacy self-management" where the law seeks to foster people's ability to make choices about their personal data. The privacy policy describes the ways that a business will collect, use, and share personal data, and people can either consent to these practices or not engage in transactions with businesses whose practices they do not find acceptable. Solove finds severe problems with this approach:

> Although privacy self-management is certainly a laudable and necessary component of any regulatory regime, I contend that it is being tasked with doing work beyond its capabilities. Privacy self-management does not provide people with meaningful control over their data. First, empirical and social science research demonstrates that there are severe cognitive problems that undermine privacy self-management. These cognitive problems impair individuals' ability to make informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal data.
>
> Second, and more troubling, even well-informed and rational individuals cannot appropriately self-manage their privacy due to several structural problems. There are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity. Moreover, many privacy harms are the result of an aggregation of pieces of data over a period of time by different entities. It is virtually impossible for people to weigh the costs and benefits of revealing information or permitting its use or transfer without an understanding of the potential downstream uses, further limiting the effectiveness of the privacy self-management framework.[35]

4. ***Visceral Notice.*** Ryan Calo argues that policymakers should explore "innovative new ways to deliver privacy notice." He contends that notice can be made more "visceral" so that people are more aware of it and understand it better. For example, a "regulation might require that a cell phone camera make a shutter sound so people know their photo is being taken."[36] Can you think of ways that privacy notices might be made more visceral? Would visceral notice address the problems that Solove has identified?

   As a related approach, there has been a discussion about "just-in-time" notice. A Staff Report from the FTC has noticed that "a disclosure (*e.g.*, "why did I get this ad?") located in close proximity to an advertisement and links to the pertinent section of a privacy policy explaining how data is collected for purposes of delivering targeted advertising, could be an effective way to communicate with consumers."[37] Is "just-in-time" notice a promising approach?

[35] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 Harv. L. Rev. 1880 (2013).

2. CONTRACT AND PROMISSORY ESTOPPEL

A privacy policy can be thought of as a type of contract, though the terms are typically dictated by the company and are non-negotiable. Consider the following advice of Scott Killingsworth to the drafters of website privacy policies:

> Considering enforcement leads to the question: what is the legal effect of a privacy policy? As between the website and the user, a privacy policy bears all of the earmarks of a contract, but perhaps one enforceable only at the option of the user. It is no stretch to regard the policy as an offer to treat information in specified ways, inviting the user's acceptance, evidenced by using the site or submitting the information. The website's promise and the user's use of the site and submission of personal data are each sufficient consideration to support a contractual obligation. Under this analysis, users would have the right to sue and seek all available remedies for breach of the privacy policy, without the need for private rights of action under such regulatory statutes as the FTC Act.[38]

Privacy policies can also be viewed simply as notices that warn consumers about the use of their personal information. Assuming that these notices are subject to change as business practices evolve, how effective are privacy policies as a means to protect privacy?

IN RE NORTHWEST AIRLINES PRIVACY LITIGATION

2004 WL 1278459 (D. Minn. 2004) (not reported in F. Supp. 2d)

MAGNUSON, J. . . . Plaintiffs are customers of Defendant Northwest Airlines, Inc. ("Northwest"). After September 11, 2001, the National Aeronautical and Space Administration ("NASA") requested that Northwest provide NASA with certain passenger information in order to assist NASA in studying ways to increase airline security. Northwest supplied NASA with passenger name records ("PNRs"),

[36] *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027 (2012).

[37] FTC Staff Report, *Self-Regulatory Principles for Online Behavioral Advertising* 35-36 (Feb. 12, 2009).

[38] Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. Intell. Prop. L. 57, 91-92 (1999).

which are electronic records of passenger information. PNRs contain information such as a passenger's name, flight number, credit card data, hotel reservation, car rental, and any traveling companions.

Plaintiffs contend that Northwest's actions constitute violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2701 *et seq.*, the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681, and Minnesota's Deceptive Trade Practices Act ("DTPA"), Minn. Stat. § 325D.44, and also constitute invasion of privacy, trespass to property, negligent misrepresentation, breach of contract, and breach of express warranties. The basis for most of Plaintiffs' claims is that Northwest's website contained a privacy policy that stated that Northwest would not share customers' information except as necessary to make customers' travel arrangements. Plaintiffs contend that Northwest's provision of PNRs to NASA violated Northwest's privacy policy, giving rise to the legal claims noted above.

Northwest has now moved to dismiss the Amended Consolidated Class Action Complaint (hereinafter "Amended Complaint"). . . .

The ECPA prohibits a person or entity from

> (1) intentionally access[ing] without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished.
>
> 18 U.S.C. § 2701(a).

Plaintiffs argue that Northwest's access to its own electronic communications service is limited by its privacy policy, and that Northwest's provision of PNRs to NASA violated that policy and thus constituted unauthorized access to the "facility through which an electronic communication service is provided" within the meaning of this section. Plaintiffs also allege that Northwest violated § 2702 of the ECPA, which states that "a person or entity providing an electronic communications service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). Northwest argues first that it cannot violate § 2702 because it is not a "person or entity providing an electronic communications service to the public." . . .

Defining electronic communications service to include online merchants or service providers like Northwest stretches the ECPA too far. Northwest is not an internet service provider. . . .

Similarly, Northwest's conduct as outlined in the Amended Complaint does not constitute a violation of § 2701. Plaintiffs' claim is that Northwest improperly disclosed the information in PNRs to NASA. Section 2701 does not prohibit improper disclosure of information. Rather, this section prohibits improper access to an electronic communications service provider or the information contained on that service provider. . . .

Finally, Northwest argues that Plaintiffs' remaining claims fail to state a claim on which relief can be granted. These claims are: trespass to property, intrusion upon seclusion, breach of contract, and breach of express warranties.

To state a claim for trespass to property, Plaintiffs must demonstrate that they owned or possessed property, that Northwest wrongfully took that property, and that Plaintiffs were damaged by the wrongful taking. Plaintiffs contend that the information contained in the PNRs was Plaintiffs' property and that, by providing that information to NASA, Northwest wrongfully took that property.

As a matter of law, the PNRs were not Plaintiffs' property. Plaintiffs voluntarily provided some information that was included in the PNRs. It may be that the information Plaintiffs provided to Northwest was Plaintiffs' property. However, when that information was compiled and combined with other information to form a PNR, the PNR itself became Northwest's property. Northwest cannot wrongfully take its own property. Thus, Plaintiffs' claim for trespass fails. . . .

Intrusion upon seclusion exists when someone "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person." . . . In this instance, Plaintiffs voluntarily provided their personal information to Northwest. Moreover, although Northwest had a privacy policy for information included on the website, Plaintiffs do not contend that they actually read the privacy policy prior to providing Northwest with their personal information. Thus, Plaintiffs' expectation of privacy was low. Further, the disclosure here was not to the public at large, but rather was to a government agency in the wake of a terrorist attack that called into question the security of the nation's transportation system. Northwest's motives in disclosing the information cannot be questioned. Taking into account all of the factors listed above, the Court finds as a matter of law that the disclosure of Plaintiffs' personal information would not be highly offensive to a reasonable person and that Plaintiffs have failed to state a claim for intrusion upon seclusion. . . .

Northwest contends that the privacy policy on Northwest's website does not, as a matter of law, constitute a unilateral contract, the breach of which entitles Plaintiffs to damages. Northwest also argues that, even if the privacy policy constituted a contract or express warranty, Plaintiffs' contract and warranty claims fail because Plaintiffs have failed to plead any contract damages. . . .

Plaintiffs' rely on the following statement from Northwest's website as the basis for their contract and warranty claims:

> When you reserve or purchase travel services through Northwest Airlines nwa.com Reservations, we provide only the relevant information required by the car rental agency, hotel, or other involved third party to ensure the successful fulfillment of your travel arrangements. . . .

The usual rule in contract cases is that "general statements of policy are not contractual." . . .

The privacy statement on Northwest's website did not constitute a unilateral contract. The language used vests discretion in Northwest to determine when the information is "relevant" and which "third parties" might need that information. Moreover, absent 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. Plaintiffs' contract and warranty claims fail as a matter of law.

Even if the privacy policy was sufficiently definite and Plaintiffs had alleged that they read the policy before giving their information to Northwest, it is likely that Plaintiffs' contract and warranty claims would fail as a matter of law. Defendants point out that Plaintiffs have failed to allege any contractual damages arising out of the alleged breach. . . .

[The case is dismissed.]

NOTES & QUESTIONS

1. ***Breach of Contract.*** In *Dyer v. Northwest Airlines Corp.,* 334 F. Supp. 2d 1196 (D.N.D. 2004), another action involving Northwest Airlines' disclosure of passenger records to the government, the court reached a similar conclusion on the plaintiffs' breach of contract claim:

> To sustain a breach of contract claim, the Plaintiffs must demonstrate (1) the existence of a contract; (2) breach of the contract; and (3) damages which flow from the breach. . . .
>
> . . . [T]he Court finds the Plaintiffs' breach of contract claim fails as a matter of law. First, broad statements of company policy do not generally give rise to contract claims. . . . Second, nowhere in the complaint are the Plaintiffs alleged to have ever logged onto Northwest Airlines' website and accessed, read, understood, actually relied upon, or otherwise considered Northwest Airlines' privacy policy. Finally, even if the privacy policy was sufficiently definite and the Plaintiffs had alleged they did read the policy prior to providing personal information to Northwest Airlines, the Plaintiffs have failed to allege any contractual damages arising out of the alleged breach.

2. ***Damages.*** 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. The court granted Jet Blue's motion to dismiss:

> 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. . . .
>
> JetBlue . . . 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. 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 (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.

If you were the plaintiffs' attorney, how would you go about establishing the plaintiffs' injury? Is there any cognizable harm when an airline violates its privacy policy by providing passenger information to the government?

3. ***Promissory Estoppel.*** Under the Restatement (Second) of Contracts § 90:

> A promise which the promisor should reasonably expect to induce action or forbearance on the part of the promisee or a third person and which does induce such action or forbearance is binding if injustice can be avoided only by enforcement of the promise. The remedy granted for breach may be limited as justice requires.

If website privacy policies are not deemed to be contracts, can they be enforced under the promissory estoppel doctrine?

4. ***Breach of Confidentiality Tort.*** Would the plaintiffs have a cause of action based on the breach of confidentiality tort?

5. ***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.[39]

6. ***Standing in Misrepresentation Claims.*** In *In re iPhone Application Litigation*, 2013 WL 6212591 (N.D. Cal. Nov. 25, 2013), plaintiffs sued Apple in a class action alleging, among other things, that Apple made misrepresentations about iPhone privacy:

> Plaintiffs claim that they relied upon Apple's representations about privacy and data collection in purchasing their iPhones. In light of Apple's statements about protecting users' privacy, Plaintiffs did not consent to the App developers transmitting Plaintiffs' information to third parties. Plaintiffs assert that as a result of Apple's misrepresentations regarding its privacy and data collection practices, Plaintiffs both overpaid for their iPhones and suffered diminishment to their iPhones' battery, bandwidth, and storage "resources."

Some of the statements Apple made in its privacy policy included:

> Your privacy is important to Apple. So we've developed a Privacy Policy that covers how we collect, use, disclose, transfer, and store your information. . . .
>
> To make sure your personal information is secure, we communicate our privacy and security guidelines to Apple employees and strictly enforce privacy safeguards within the company. . . .
>
> Apple takes precautions—including administrative, technical, and physical measures—to safeguard your personal information against loss, theft, and misuse as well as against unauthorized access, disclosure, alteration, and destruction. . . .

The court held:

> While the iDevice Plaintiffs identify numerous purported misrepresentations and argue that they relied on them in purchasing their iPhones the evidentiary record is devoid of "specific facts" to support Plaintiffs' assertions. Critically, *none* of the Plaintiffs presents evidence that he or she even saw, let alone read and relied upon, the alleged misrepresentations contained in the Apple Privacy Policies . . . or App Store Terms and Conditions, either prior to purchasing his or her iPhone, or at any time thereafter.
>
> In their depositions, Plaintiffs either could not recall having read any of these policies (or any other Apple representation) in connection with obtaining their iPhones, or expressly disavowed having read any Apple policy, or anything else about the iPhone, prior to purchasing one.

The court further reasoned:

[39] Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 Penn. St. L. Rev. 587, 612, 618 (2007).

> First, Plaintiffs suggest that standing is established as long as a plaintiff "receives" a misrepresentation. The implication of this argument seems to be that a plaintiff can show standing as long as the defendant has disseminated the alleged misrepresentation to her in some fashion, regardless of whether the plaintiff ever actually sees, reads, or hears the defendant's statement. The Court questions how one can act in reliance on a statement one does not see, read, or hear. . . .
>
> Second, Plaintiffs argue that the Court should infer reliance from the fact that Plaintiffs had iTunes accounts and therefore had to, at some point, agree to Apple's Terms and Conditions and Privacy Policy. . . . [B]y virtue of having active iTunes accounts, Plaintiffs would have been asked to agree to Apple's updated Privacy Policy at some point during the class period. . . . Plaintiffs ask the Court to infer that Plaintiffs must have read and relied on misrepresentations contained in Apple's Privacy Policy at some point during the class period.
>
> There are two problems with this theory. Most critically, it has no evidentiary support. No Plaintiff, in either a deposition or declaration, identified an Apple Privacy Policy as the source of his or her "understanding" regarding Apple's policies concerning privacy and data collection. . . .
>
> What is more, the mere fact that Plaintiffs had to scroll through a screen and click on a box stating that they agreed with the Apple Privacy Policy in July 2010 does not establish, standing alone, that Plaintiffs actually read the alleged misrepresentations contained in that Privacy Policy, let alone that these misrepresentations subsequently formed the basis for Plaintiffs' "understanding" regarding Apple's privacy practices. Accordingly, the existence of Plaintiffs' iTunes accounts does not, *by itself*, demonstrate that Plaintiffs actually read and relied on any misrepresentations contained in the updated Privacy Policy from July 2010.

7. ***Promises of Anonymity.*** In *Saffold v. Plain Dealer Publishing Co.*, a state court judge (Shirley Strickland Saffold) sued the *Cleveland Plain Dealer* for stating that comments posted on the newspaper's website under the screen name "lawmiss" originated from a computer used by the judge and her daughter. Some of these comments related to cases before Judge Saffold. Judge Saffold claimed that the newspaper's disclosure of the identity of "lawmiss" violated its website's privacy policy, which stated that "personally identifiable information is protected." Moreover, the user agreement that was part of the registration process to create an account on the website incorporated the privacy policy. The case was settled before any judicial decision was issued. Suppose, however, the litigation had proceeded. Would Judge Saffold have a claim for breach of contract or promissory estoppel?
8. ***Website Communities and Promissory Estoppel.*** Consider Woodrow Hartzog:

> Suppose a person improperly provides others with access to a friend's Facebook profile. Suppose a member of a dating website copies another's dating profile and discloses the information to the general public. Or suppose a member of an online support community for recovering alcoholics reveals the names and other personal information of other members. Should members of an online community be able to expect and legally enforce the confidentiality of their data? . . .

> I contend that the law can ensure confidentiality for members of online communities through promissory estoppel. . . .
>
> One of the immediate difficulties with using promissory estoppel is that members of online communities have not made agreements between each other. They have merely agreed to the terms of use of the website and community. Suppose Member A of an online community discloses the private information of Member B. Would Member B be able to sue Member A for promissory estoppel even though Member A never made a direct promise to Member B?
>
> In order to allow all users within the community the ability to rely on promises of confidentiality, I propose application of either the third-party beneficiary doctrine or the concept of dual agency effectuated through a website's terms of use. Although the implementation of promissory estoppel in this context would be challenging, I conclude that the promissory estoppel theory for confidential disclosure could have positive practical effects and advance both privacy and free speech objectives.[40]

What are the pros and cons of Hartzog's proposal? Should members of online communities have any obligations to each other?

9. ***Are Website Privacy Settings Part of a Contract?*** Woodrow Hartzog contends that website privacy settings and other design features should be considered as part of the contract between the website and the user:

> When courts seek to determine a website user's privacy expectations and the website's promises to that user, they almost invariably look to the terms of use agreement or to the privacy policy. They rarely look to the privacy settings or other elements of a website where users specify their privacy preferences. These settings and elements are typically not considered to be part of any contract or promise to the user. Yet studies have shown that few users actually read or rely upon terms of service or privacy policies. In contrast, users regularly take advantage of and rely upon privacy settings. . . . [T]o the extent website design is incorporated into or consistent with a website's terms of use, or to the extent website design induces reliance, courts should consider these design features as enforceable promises.[41]

Facebook and other social media websites, for example, have privacy settings that allow users to establish how broadly their information will be shared. If Facebook were to expose a person's information more broadly than he set it in his privacy settings, could that be the basis of a contract or promissory estoppel lawsuit? What other design elements might be considered part of a website's contract or promise with a user?

10. ***Contract and Morality***. In Canada, Gabrielle Nagy sued her cellphone company, Rogers Communications, for breach of contract when it incorporated her cell phone bill into the family phone bill. The result was that her husband discovered that she was frequently calling another man. Nagy eventually confessed to her husband that she was having an affair, and they divorced. Consider David Hoffman:

[40] Woodrow Hartzog, *Promises and Privacy: Promissory Estoppel and Confidential Disclosure in Online Communities*, 82 Temp. L. Rev. 891, 893-96 (2009).

[41] Woodrow Hartzog, *Website Design as Contract,* 60 Am. U. L. Rev. 1635 (2011).

> I think the breach of contract lawsuit, if filed in an American court applying fairly ordinary domestic contract principles, would be a loser. . . .
>
> The common law generally dislikes punishing breach with liability or damages when the inevitable consequence of performance is to motivate socially wrongful conduct, and nonperformance to retard it. . . .
>
> What about cases where A and B contract not to disclose some fact X, and the nondisclosure will create harm for innocent third parties. These contracts are often enforced (every confidentiality clause probably shelters some fact with the potential for third party harm). But the degree to which the nonbreaching party can recover ought to turn on what's being kept secret: if the secret is particularly socially harmful (oozing toxic sludge!) we might believe that the hiding, non-breaching, party doesn't get to recover for breach. Thus, you sometimes see cases where fraud-revealing employees are protected from consequences of nondisclosure agreements by (effectively) common law whistleblower doctrines.
>
> Where the third-party harm *relates to marriage*, the law appears to be more categorical. Public policy concerns about contracting and third party harm are strongest in agreements touching on issues of family life and infidelity.[42]

Is Hoffman correct that such a breach of contract case would lose under American law? Should courts choose which contracts to enforce based on morality? If a company breaches a contract and reveals that a person is doing something immoral, should that breach go unremedied?

11. ***Interpreting Promises.*** In *In re iPhone Application Litigation*, 844 F. Supp. 2d 1040 (N.D. Cal. June 12, 2012), plaintiffs sued Apple for the practices of third-party apps. Apple argued that its Privacy Policy and Terms of Use disclaimed liability from third-party conduct. However, the court concluded:

> Additionally, to the extent that Apple argues that it has no duty to review or evaluate apps and that it has disclaimed any liability arising from the actions of third parties, this argument both ignores contradictory statements made by Apple itself, and the allegations asserted by Plaintiffs regarding Apple's own conduct with respect to the alleged privacy violations. For one, it is not clear that Apple disclaimed all responsibility for privacy violations because, while Apple claimed not to have any liability or responsibility for any third party materials, websites or services, Apple also made affirmative representations that it takes precautions to protect consumer privacy. Additionally, Plaintiffs' allegations go beyond asserting that Apple had a duty to review or police third party apps. Instead, Plaintiffs allege Apple was responsible for providing user's information to third parties. Plaintiffs allege that Apple is independently liable for any statutory violations that have occurred. At the motion to dismiss stage, then, the Court is not prepared to rule that the Agreement establishes an absolute bar to Plaintiffs' claims.

The court recognized that increased security risks and lessened device resources (storage, battery life, and bandwidth) from third-party apps could constitute concrete injuries.

[42] David Hoffman, *Contracts and Privacy,* Concurring Opinions (June 21, 2010), http://www.concurringopinions.com/archives/2010/06/contracts-and-privacy.html.

Should a more general statement that a company protects privacy override more specific statements such as disclaiming responsibility for third-party apps? Or should the more specific statements govern over the more general ones? Suppose a company's founder in an interview states: "We care deeply about our the privacy of our customers and protect it zealously." Could this trump a statement in the privacy policy that allows personal data to be shared with third parties unless people opt out?

12. ***The Cost of "Free".*** Many online services, such as Google and Facebook, are free. Chris Hoofnagle and Jan Whittington argue that these services are not really free:

> [C]onceiving of transactions as free can harm both consumers and competition. These exchanges often carry a hidden charge: the forfeit of one's personal information. The service provider may expect to earn revenues from the personal information collected about consumers who devote their attention to advertising and other services, such as games, from third parties. The more time the consumer spends using the service and revealing information, the more the service can adjust the product to reveal more information about the consumer and tailor its advertising of products to that consumer's personal information.[43]

Hoofnagle and Wittington contend that many "information-intensive companies misuse the term 'free' to promote products and services that incur myriad hidden, nonpecuniary costs." What are the implications of recognizing that consumers are paying a price for sharing their personal data? To what extent does this fact affect contract law analysis when it comes to privacy policies?

D. PROPERTY LAW

A number of commentators propose that privacy can be protected by restructuring the property rights that people have in personal information. For example, according to Richard Murphy, personal information "like all information, is property." He goes on to conclude:

> . . . [I]n many instances, privacy rules are in fact implied contractual terms. To the extent that information is generated through a voluntary transaction, imposing nondisclosure obligations on the recipient of the information may be the best approach for certain categories of information. The value that information has ex post is of secondary importance; the primary question is what is the efficient contractual rule. Common-law courts are increasingly willing to impose an implied contractual rule of nondisclosure for many categories of transactions, including those with attorneys, medical providers, bankers, and accountants. Many statutes can also be seen in this light — that is, as default rules of privacy.

[43] Chris Jay Hoofnagle and Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. Rev. 606 (2014).

> And an argument can be made for the efficiency of a privacy default rule in the generic transaction between a merchant and a consumer.[44]

Lawrence Lessig also contends that privacy should be protected with property rights. He notes that "[p]rivacy now is protected through liability rules — if you invade someone's privacy, they can sue you and you must then pay." A "liability regime allows a taking, and payment later." In contrast, a property regime gives "control, and power, to the person holding the property right." Lessig argues: "When you have a property right, before someone takes your property they must negotiate with you about how much it is worth."[45]

Jerry Kang proposes a type of fusion between property and contract regulation when he proposes that there be a default rule that individuals retain control over information they surrender during Internet transactions. He contends that this default rule is more efficient than a default rule where companies can use the data as they see fit. The default rule that Kang proposes could be bargained around: "With this default, if the firm valued personal data more than the individual, then the firm would have to buy permission to process the data in functionally unnecessary ways."[46] In essence, Kang is creating a property right in personal data, and people could sell the right to use it to companies.

Other commentators critique the translation of privacy into a form of property right that can be bartered and sold. For example, Katrin Schatz Byford argues that viewing "privacy as an item of trade . . . values privacy only to the extent it is considered to be of personal worth by the individual who claims it." She further contends: "Such a perspective plainly conflicts with the notion that privacy is a collective value and that privacy intrusions at the individual level necessarily have broader social implications because they affect access to social power and stifle public participation."[47]

Consider Pamela Samuelson's argument as to why property rights are inadequate to protect privacy:

> . . . Achieving information privacy goals through a property rights system may be difficult for reasons other than market complexities. Chief among them is the difficulty with alienability of personal information. It is a common, if not ubiquitous, characteristic of property rights systems that when the owner of a property right sells her interest to another person, that buyer can freely transfer to third parties whatever interest the buyer acquired from her initial seller. Free alienability works very well in the market for automobiles and land, but it is far from clear that it will work well for information privacy. . . . Collectors of data may prefer a default rule allowing them to freely transfer personal data to whomever they wish on whatever terms they can negotiate with their future buyers. However, individuals concerned with information privacy will generally want a default rule prohibiting retransfer of the data unless separate permission is

[44] Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Geo. L.J. 2381, 2416-17 (1996).

[45] Lawrence Lessig, *Code and Other Laws of Cyberspace* (1999).

[46] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193 (1998).

[47] Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 Rutgers Computer & Tech. L.J. 1 (1998). For an argument about the problems of commodifying certain goods and of viewing all human conduct in light of the market metaphor, see Margaret Jane Radin, *Contested Commodities* (1996).

> negotiated. They will also want any future recipient to bind itself to the same constraints that the initial purchaser of the data may have agreed to as a condition of sale. Information privacy goals may not be achievable unless the default rule of the new property rights regime limits transferability. . . .
>
> . . . From a civil liberties perspective, propertizing personal information as a way of achieving information privacy goals may seem an anathema. Not only might it be viewed as an unnecessary and possibly dangerous way to achieve information privacy goals, it might be considered morally obnoxious. If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights. . . .[48]

Daniel Solove also counsels against protecting privacy as a form of property right because the "market approach has difficulty assigning the proper value to personal information":

> . . . [T]he aggregation problem severely complicates the valuation process. An individual may give out bits of information in different contexts, each transfer appearing innocuous. However, the information can be aggregated and could prove to be invasive of the private life when combined with other information. It is the totality of information about a person and how it is used that poses the greatest threat to privacy. As Julie Cohen notes, "[a] comprehensive collection of data about an individual is vastly more than the sum of its parts." From the standpoint of each particular information transaction, individuals will not have enough facts to make a truly informed decision. The potential future uses of that information are too vast and unknown to enable individuals to make the appropriate valuation. . . .
>
> [Property rights] cannot work effectively in a situation where the power relationship and information distribution between individuals and public and private bureaucracies is so greatly unbalanced. In other words, the problem with market solutions is not merely that it is difficult to commodify information (which it is), but also that a regime of default rules alone (consisting of property rights in information and contractual defaults) will not enable fair and equitable market transactions in personal information. . . .[49]

In contrast to these skeptics, Paul Schwartz develops a model of propertized personal data that would help fashion a market for data trade that would respect individual privacy and help maintain a democratic order. Schwartz calls for "limitations on an individual's right to alienate personal information; default rules that force disclosure of the terms of trade; a right of exit for participants in the market; the establishment of damages to deter market abuses; and institutions to police the personal information market and punish privacy violations." In his judgment, a key element of this model is its approach of "hybrid inalienability" in which a law allows individuals to share their personal information, but also places limitations on future use of the information. Schwartz explains:

> This hybrid consists of a use-transferability restriction plus an opt-in default. In practice, it would permit the transfer for an initial category of use of personal data, but only if the customer is granted an opportunity to block further transfer or use

[48] Pamela Samuelson, *Privacy as Intellectual Property?*, 52 Stan. L. Rev. 1125, 1137-47 (2000).

[49] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393 (2001).

> by unaffiliated entities. Any further use or transfer would require the customer to opt in — that is, it would be prohibited unless the customer affirmatively agrees to it.
>
> As an initial example concerning compensated telemarketing, a successful pitch for Star Trek memorabilia would justify the use of personal data by the telemarketing company and the transfer of it both to process the order and for other related purposes. Any outside use or unrelated transfers of this information would, however, require obtaining further permission from the individual. Note that this restriction limits the alienability of individuals' personal information by preventing them from granting one-stop permission for all use or transfer of their information. A data processor's desire to carry out further transfers thus obligates the processor to supply additional information and provides another chance for the individual to bargain with the data collector. . . .
>
> To ensure that the opt-in default leads to meaningful disclosure of additional information, however, two additional elements are needed. First, the government must have a significant role in regulating the way that notice of privacy practices is provided. As noted above, a critical issue will be the "frame" in which information about data processing is presented. . . .
>
> Second, meaningful disclosure requires addressing what Henry Hansmann and Reinier Kraakman term "verification problems." Their scholarship points to the critical condition that third parties must be able to verify that a given piece of personal information has in fact been propertized and then identify the specific rules that apply to it. As they explain, "[a] verification rule sets out the conditions under which a given right in a given asset will run with the asset." In the context of propertized personal information, the requirement for verification creates a role for nonpersonal metadata, a tag or kind of barcode, to provide necessary background information and notice.[50]

Finally, consider what Warren and Brandeis said about privacy as a property claim:

> The aim of [copyright] statutes is to secure to the author, composer, or artist the entire profits arising from publication. . . .
>
> But where the value of the production is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all, it is difficult to regard the right as one of property, in the common acceptation of that term.[51]

E. FTC SECTION 5 ENFORCEMENT

Beyond private law actions such as contract and promissory estoppel, the promises that companies make regarding their privacy practices can be enforced by the government through public law. Private law actions are initiated on behalf of harmed individuals, who can obtain monetary or other redress for their injuries.

[50] Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 Harv. L. Rev. 2055, 2056, 2098-99 (2004). *See also* Vera Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. Davis L. Rev. 379 (2003) (although a collector may have rights in individuals' personal information, a property approach would correctly subordinate these rights to the rights of the individuals).

[51] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

In contrast, public law actions are initiated by government agencies or officials, and they typically involve fines and penalties.

In 1995, Congress and privacy experts first asked the Federal Trade Commission (FTC) to become involved with consumer privacy issues. Since 1998, the FTC has maintained the position that the use or dissemination of personal information in a manner contrary to a posted privacy policy is a deceptive practice under the FTC Act, 15 U.S.C. § 45.

The Act prohibits "unfair or deceptive acts or practices in or affecting commerce." § 45(n).

Deception. A deceptive act or practice is a material "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[52]

Unfairness. The FTC Act classifies a trade practice as unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n). Actions of a company can be both deceptive and unfair.

The Scope of Section 5. Section 5 provides very broad jurisdiction to the FTC. However, the FTC does not have jurisdiction over all companies. Exempt from the FTC's jurisdiction are many types of financial institutions, airlines, telecommunications carriers, and other types of entities. § 45(a)(2). Additionally, non-profit institutions such as schools are often not covered.

The FTC's Structure. The FTC is headed by five commissioners, who are appointed by the President and confirmed by the Senate. They each serve a seven-year term. The commissioners must be a bipartisan group — no more than three can be members of the same political party. One of the commissioners is designated by the President as chairman.

Enforcement. The FTC can obtain injunctive remedies. § 53. The Act does not provide for private causes of action; only the FTC can enforce the Act. The FTC does not have the ability to issue fines for violations of Section 5, but the FTC can issue fines when companies violate a consent decree previously entered into for a violation of Section 5.

Rulemaking. The FTC lacks practical rulemaking authority under Section 5. The FTC has only Magnuson-Moss rulemaking authority, which is highly burdensome as a procedural matter. According to Beth DeSimone and Amy Mudge:

> Right now, the FTC is constrained in its rulemaking by the so-called "Magnuson-Moss" rules. These rules require the FTC Staff to engage in an industry-wide investigation, prepare draft staff reports, propose a rule, and engage in a series of public hearings, including cross-examination opportunities prior to issuing a final rule in any area. These processes are so burdensome that the FTC has not engaged in a Magnuson-Moss rule-making in 32 years.[53]

[52] Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce (Oct. 14, 1983).

The Growing Role of the FTC. Since it began enforcing the FTC Act for breaches of privacy policies in 1998, the FTC has brought a number of actions, most of which have settled. The FTC has brought about 170 privacy and data security actions under Section 5, averaging about 10 per year, though the number per year has increased throughout the years.

According to Daniel Solove and Woodrow Hartzog:

> Despite over fifteen years of FTC enforcement, there are hardly any judicial decisions to show for it. The cases have nearly all resulted in settlement agreements. Nevertheless, companies look to these agreements to guide their decisions regarding privacy practices. Those involved with helping businesses comply with privacy law—from chief privacy officers to inside counsel to outside counsel—parse and analyze the FTC's settlement agreements, reports, and activities as if they were pronouncements by the Chairman of the Federal Reserve. Thus, in practice, FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States—more so than nearly any privacy statute or common law tort.[54]

Companies that violate settlement orders are liable for a civil penalty of up to $16,000 for each violation. Injunctive or other equitable relief is also available.

FTC Privacy Enforcement Beyond Section 5. Beyond Section 5, the FTC also enforces the Gramm-Leach-Bliley Act (GLBA) and the Children's Online Privacy Protection Act (COPPA). Additionally, it enforces the US-EU Safe Harbor Arrangement. The FTC used to be the primary enforcer of the Fair Credit Reporting Act (FCRA), but that responsibility has largely been passed to the Consumer Financial Protection Bureau (CFPB). The FTC still retains some limited enforcement power over FCRA that is shared with CFPB. Although the FTC cannot issue fines under Section 5, it has the power to issue fines under the GLBA, COPPA, and FCRA.

IN THE MATTER OF SNAPCHAT, INC.

2014 WL 1993567 (FTC May 8, 2014)

COMPLAINT

The Federal Trade Commission, having reason to believe that Snapchat, Inc. ("respondent") has violated the provisions of the Federal Trade Commission Act,

[53] Beth DeSimone & Amy Mudge, *Is Congress Putting the FTC on Steroids?*, Seller Beware Blog, Arnold & Porter (Apr. 26, 2010), http://www.consumeradvertisinglawblog.com/2010/04/is-congress-putting-the-ftc-on-steroids.html.

[54] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 Colum. L. Rev. 583, 585-86 (2014).

and it appearing to the Commission that this proceeding is in the public interest, alleges: . . . .

3. Snapchat provides a mobile application that allows consumers to send and receive photo and video messages known as "snaps." Before sending a snap, the application requires the sender to designate a period of time that the recipient will be allowed to view the snap. Snapchat markets the application as an "ephemeral" messaging application, having claimed that once the timer expires, the snap "disappears forever." . . .

6. Snapchat marketed its application as a service for sending "disappearing" photo and video messages, declaring that the message sender "control[s] how long your friends can view your message." Before sending a snap, the application requires the sender to designate a period of time — with the default set to a maximum of 10 seconds — that the recipient will be allowed to view the snap. . .

8. From October 2012 to October 2013, Snapchat disseminated, or caused to be disseminated, to consumers the following statement on the "FAQ" page on its website:

> Is there any way to view an image after the time has expired?
>
> No, snaps disappear after the timer runs out. . . .

9. Despite these claims, several methods exist by which a recipient can use tools outside of the application to save both photo and video messages, allowing the recipient to access and view the photos or videos indefinitely.

10. For example, when a recipient receives a video message, the application sstores the video file in a location outside of the application's "sandbox" (*i.e.*, the application's private storage area on the device that other applications cannot access). Because the file is stored in this unrestricted area, until October 2013, a recipient could connect his or her mobile device to a computer and use simple file browsing tools to locate and save the video file. This method for saving video files sent through the application was widely publicized as early as December 2012. Snapchat did not mitigate this flaw until October 2013, when it began encrypting video files sent through the application.

11. Furthermore, third-party developers have built applications that can connect to Snapchat's application programming interface ("API"), thereby allowing recipients to log into the Snapchat service without using the official Snapchat application. Because the timer and related "deletion" functionality is dependent on the recipient's use of the official Snapchat application, recipients can instead simply use a third-party application to download and save both photo and video messages. . . .

14. Snapchat claimed that if a recipient took a screenshot of a snap, the sender would be notified. . . .

15. However, recipients can easily circumvent Snapchat's screenshot detection mechanism. For example, on versions of iOS prior to iOS 7, the recipient need only double press the device's Home button in rapid succession to evade the detection mechanism and take a screenshot of any snap without the sender being notified. This method was widely publicized.

16. As described in Paragraphs 6, 7, and 8, Snapchat has represented, expressly or by implication, that when sending a message through its application, the message will disappear forever after the user-set time period expires.

17. In truth and in fact, as described in Paragraph 9-12, when sending a message through its application, the message may not disappear forever after the user-set time period expires. Therefore, the representation set forth in Paragraph 16 is false or misleading.

18. As described in Paragraphs 7 and 14, Snapchat has represented, expressly or by implication, that the sender will be notified if the recipient takes a screenshot of a snap.

19. In truth and in fact, as described in Paragraph 15, the sender may not be notified if the recipient takes a screenshot of a snap. Therefore, the representation set forth in Paragraph 18 is false or misleading. . . .

20. From June 2011 to February 2013, Snapchat disseminated or caused to be disseminated to consumers the following statements in its privacy policy:

> We do not ask for, track, or access any location-specific information from your device at any time while you are using the Snapchat application.

21. In October 2012, Snapchat integrated an analytics tracking service in the Android version of its application that acted as its service provider. While the Android operating system provided notice to consumers that the application may access location information, Snapchat did not disclose that it would, in fact, access location information, and continued to represent that Snapchat did "not ask for, track, or access any location-specific information . . . ."

22. Contrary to the representation in Snapchat's privacy policy, from October 2012 to February 2013, the Snapchat application on Android transmitted Wi-Fi-based and cell-based location information from users' mobile devices to its analytics tracking service provider. . . .

AGREEMENT CONTAINING CONSENT ORDER

The Federal Trade Commission ("Commission") has conducted an investigation of certain acts and practices of Snapchat, Inc. ("Snapchat" or "proposed respondent"). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between Snapchat, Inc., by its duly authorized officers, and counsel for the Federal Trade Commission that: . . .

2. Proposed respondent neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in this order. Only for purposes of this action, proposed respondent admits the facts necessary to establish jurisdiction. . . .

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or indirectly, shall not misrepresent in any manner, expressly or by implication, in or affecting commerce, the extent to which respondent or its products or services maintain and protect the privacy, security, or confidentiality of any covered information, including but not limited to: (1) the extent to which a message is deleted after being viewed by the recipient; (2) the extent to which

respondent or its products or services are capable of detecting or notifying the sender when a recipient has captured a screenshot of, or otherwise saved, a message; (3) the categories of covered information collected; or (4) the steps taken to protect against misuse or unauthorized disclosure of covered information.

IT IS FURTHER ORDERED that respondent, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information, whether collected by respondent or input into, stored on, captured with, or accessed through a computer using respondent's products or services. Such program, the content and implementation of which must be fully documented in writing, shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information, including:

A. the designation of an employee or employees to coordinate and be accountable for the privacy program;

B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in the respondent's unauthorized collection, use, or disclosure of covered information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order; and (2) product design, development and research;

C. the design and implementation of reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of the privacy controls and procedures;

D. the development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards;

E. the evaluation and adjustment of respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows, or has reason to know, may have a material impact on the effectiveness of its privacy program.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. . . .

This order will terminate twenty (20) years from the date of its issuance. . . .

NOTES & QUESTIONS

1. ***FTC Consent Decrees.*** When FTC cases are settled, the complaint and consent decree are typically issued together. The complaint is not released during the investigation or settlement negotiations.

   FTC consent decrees often contain at least some of the following elements: (1) prohibition on the activities in violation of the FTC Act; (2) steps to remediate the problematic activities, such as software patches or notice to consumers; (3) deletion of wrongfully-obtained consumer data; (4) modifications to privacy policies; (5) establishment of a comprehensive privacy program, including risk assessment, appointment of a person to coordinate the program, and employee training, among other things; (6) biennial assessment reports by independent auditors; (7) recordkeeping to facilitate FTC enforcement of the order; (8) obligation to alert the FTC of any material changes in the company that might affect compliance obligations (such as mergers or bankruptcy filings).
2. ***Types of Section 5 Privacy and Security Violations.*** What are the types of cases the FTC brings? Under the "deception" prong of its authority, the FTC brings cases for broken promises of privacy, general deception, insufficient notice, and unreasonable data security practices. Under the "unfairness" prong, the FTC brings cases for retroactive changes to privacy policies, deceitful data collection, improper use of data, unfair design or unfair default settings, and unfair data security practices.[55]
3. ***Broken Promises and Deception.*** Snapchat represents a classic privacy deception case, where a company is found to be in violation of promises it makes in its privacy policy. Recall the definition of a deceptive practice: it is a material "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumers' detriment." Can the FTC bring a deception action for statements that are not made in a company's privacy policy? Suppose the founder of a company states in an interview that her company will never provide consumer data to a third party. This statement contradicts the company's own privacy policy, which correctly indicates that the company does provide consumer to data to certain third parties. Could the founder's statement be the basis of an FTC action for deception?
4. ***FTC Enforcement: A Slap on the Wrist?*** The FTC does not have the power to issue fines under Section 5. The FTC can issue fines if enforcing other statutory regimes that permit such monetary sanctions, such as the GLBA.

   Does the FTC have sufficient enforcement teeth to deter companies from engaging in privacy violations? To what extent does the FTC's settlement with Snapchat require more than complying appropriately with the law in the future?

   Farhad Manjoo, in commenting on Snapchat notes that FTC consent agreements "have become something of a rite of passage for tech companies." He goes on to argue:

---

[55] Solove & Hartzog, *FTC and the New Common Law of Privacy, supra.*

> But there is little evidence that these agreements have led to a wholesale shift in how tech companies handle private data. While the F.T.C. deals might push the companies to be more careful about privacy changes, being careful is not the same as being private. It's possible — and seems likely — that agreements with the government serve mainly to add a veneer of legitimacy over whatever moves the companies planned to make anyway.[56]

Manjoo also comments on a case where the FTC found that Google violated a 2011 consent decree that Google made with the FTC. The FTC issued the largest-ever fine against a company. Manjoo writes:

> How much was that record-setting fine? $22.5 million. Note that in 2012, Google made a profit of $10.7 billion, most of it through advertising that was based in some way on data it collected from users. If you do the math, the agency's fine represented about 0 percent of Google's income that year.[57]

One aspect of the settlement to note is that the consent order lasts for 20 years. This is quite a long period of time. In comparison, an HHS consent order typically lasts for 1 to 3 years. Is 20 years too long? Or appropriate?

5. ***If People Do Not Read Privacy Policies, Why Enforce Them?*** Daniel Solove points out that people rarely read privacy policies:

> Most people do not read privacy notices on a regular basis. As for other types of notices, such as end-user license agreements and contract boilerplate terms, studies show only a miniscule percentage of people read them. Moreover, few people opt out of the collection, use, or disclosure of their data when presented with the choice to do so. Most people do not even bother to change the default privacy settings on websites.[58]

Why should the FTC enforce privacy policies if people do not read them? Solove points out that privacy policies are often difficult for consumers to understand and there is a tradeoff between making policies understandable and providing sufficient detail to explain the complex ways personal data is used and protected:

> The evidence suggests that people are not well informed about privacy. Efforts to improve education are certainly laudable, as are attempts to make privacy notices more understandable. But such efforts fail to address a deeper problem — privacy is quite complicated. This fact leads to a tradeoff between providing a meaningful notice and providing a short and simple one.

Privacy policies not only serve to inform consumers; they also serve to inform privacy advocates and regulators, and they are a way to hold companies

[56] Farhad Manjoo, *Another Tech Company Finds the F.T.C. Looking Over Its Shoulder*, N.Y. Times Bits Blog, May 8, 2014, http://bits.blogs.nytimes.com/2014/05/08/will-a-government-settlement-improve-snapchats-privacy-dont-count-on-it/.

[57] *Id.* Editors' Note: the 0 percent estimation may seem surprising. But in 2012, Google reported $10.74 billion in total profits. That year, online advertising accounted for about 95 percent of Google's profits. Ninety-five percent of $10.74 billion is approximately $10.203 billion. A $22.5 million dollar fine represents 0.002205 percent of Google profits. Hence, a 0 percent estimation follows normal rounding conventions.

[58] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 Harv. L. Rev. 1880 (2013).

to their word. But if experts are the audience for privacy policies, then doesn't this conflict with the needs of the consumer audience, for whom simpler is better?

6. ***Why Did the FTC Become the Leading U.S. Privacy Agency?*** In 2000, Steven Hetcher assessed the FTC's behavior in enforcing privacy in these terms:

> By the Agency's lights, its promotion of the fair practice principles should satisfy privacy advocates, as the fair information practice principles are derived from pre-existing norms of the advocacy community. Public interest advocates contend to the contrary, however, that privacy policies ill serve their aspirational privacy norms. They argue that privacy policies are typically not read by website users. They are written in legalese such that even if people read them, they will not understand them. Hence, they do not provide notice and thus cannot lead to consent. In addition, there is evidence that many sites do not adhere to their own policies. The policies are subject to change when companies merge, such that one company's policy is likely to go unheeded. Finally, very few privacy policies guarantee security or enforcement. Thus, the provision of a privacy policy by a website does not automatically promote the fair practice principles.
>
> Despite these problems, the FTC has strongly endorsed privacy policies. This raises a question as to why the Agency should do so, given the severe criticism privacy policies have received. Why, for instance, is the FTC not coming out in support of the creation of a new agency to oversee privacy protection? . . .
>
> There is a public choice answer as to why the Agency has promoted privacy policies, despite their problems (and despite the fact that they do not appear to promote the interests of any industry groups whose favor the FTC might be seeking). It is through privacy policies that the FTC is gaining jurisdiction over the commercial Internet. Jurisdiction is power. In other words, the FTC acts as if it has a plan to migrate its activities to the Internet, and privacy policies have been at the core of this plan. . . .[59]

After the writings by Hetcher, however, the FTC developed an additional role — the agency began to enforce standards of data security. Does this role fit in with Hetcher's analysis ("through privacy policies . . . the FTC is gaining jurisdiction over the commercial Internet")?

7. ***The Scope of the FTC's Power.*** How much power does Section 5 provide to the FTC to regulate the way companies collect, use, and share personal data? In *FTC v. Wyndham Worldwide Corp.*, 10 F.Supp.3d 602 (D.N.J. 2014), Wyndham Hotels challenged the scope of the FTC's power.

The *Wyndham* case arose from a series of data breaches suffered by Wyndham. In its complaint against Wyndham, the FTC alleged a variety of poor data security practices by Wyndham that led to the breaches. Although the case involves data security and is excerpted and discussed in more depth in Chapter 10, the arguments in the case could apply to the FTC's privacy enforcement. One of the arguments made by Wyndham was that because

[59] Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 Vand. L. Rev. 2041 (2000). *See also* Steven Hetcher, *Norms in a Wired World* (2004); Steven Hetcher, *Changing the Social Meaning of Privacy in Cyberspace*, 15 Harv. J.L. & Tech. 149 (2001); Steven A. Hetcher, *Norm Proselytizers Create a Privacy Entitlement in Cyberspace*, 16 Berkeley Tech. L.J. 877 (2001).

Congress enacted targeted data security legislation elsewhere, yet failed to create a statute explicitly authorizing the FTC to regulate data security, the FTC lacked the power to regulate. The court rejected this argument, concluding that the FTC's Section 5 power is very broad and that the context-specific data security statutes simply enhance data security protection in certain contexts. The court concluded that Wyndham "fails to explain how the FTC's unfairness authority over data security would lead to a result that is incompatible with more recent legislation and thus would 'plainly *contradict* congressional policy.' "

As Hartzog and Solove argue: "Congress gave the FTC very broad and general regulatory authority by design to allow for a more nimble and evolutionary approach to the regulation of consumer protection." They contend that normatively the FTC's broad power is justified and that "the FTC not only should have broad data protection enforcement powers, but that it also should be exercising these powers more robustly. The FTC should enforce more expansively, embrace consensus norms more quickly, and take more of a leadership role in the development of privacy norms and standards."[60] Should the FTC take an even greater role and more aggressively try to develop privacy norms?

8. ***Are FTC Consent Decrees Similar to Common Law?*** Daniel Solove and Woodrow Hartzog argue that the body of FTC consent decrees has some key similarities to common law. "Practitioners look to FTC settlements as though they have precedential weight. The result is that lawyers consult and analyze these settlements in much the same way as they do judicial decisions."
9. ***Fair Notice.*** Some commentators critique the FTC for failing to articulate its standards clearly enough. In the context of the FTC's data security cases, Gerard Stegmaier and Wendell Bartnick argue:

> The FTC's current practice. . . relies heavily upon the publication of negotiated resolutions that consist of draft complaints coupled with consent agreements, as well as the release of reports and other interpretive guidance that blend best practices with law. The result is that legal requirements are generally shrouded in mystery and uncertain risk of enforcement discretion. Finally, . . . a standard based on "reasonableness" grounded solely in settlements raises its own questions of whether constitutionally adequate fair notice was provided. Such a standard seems unfair and problematic to those tasked with assisting entities in avoiding unfair and deceptive trade practices.[61]

In another case, LabMD challenged the FTC with an argument quite similar to Stegmaier and Bartnick's. Writing for the FTC in denying LabMD's motion to dismiss, Commissioner Wright stated:

> LabMD's due process claim is particularly untenable when viewed against the backdrop of the common law of negligence. Every day, courts and juries subject companies to tort liability for violating uncodified standards of care, and the

[60] Woodrow Hartzog & Daniel J. Solove, T*he Scope and Potential of FTC Data Protection*, 83 Geo. Wash. L. Rev. 2230 (2015).

[61] Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 Geo. Mason L. Rev. 673 (2013).

> contexts in which they make those fact-specific judgments are as varied and fast-changing as the world of commerce and technology itself.

Hartzog and Solove contend:

> In a common law system — or any system where matters are decided case-by-case and there is an attempt at maintaining consistency across decisions, any reasonableness standard will evolve into something more akin to a rule with specifics over time. Indeed, any broad standard will follow this evolutionary trajectory. . . .
>
> While some initial uncertainty might be the present at the outset, the clarity provided by each additional legal action virtually guarantees ever increasing determinism for those already charged with a reasonable adherence to commonly shared industry standards.
>
> The FTC is not exceeding its authority because this developmental pattern is practically inevitable and quite predictable given the clarity offered by incorporation of generally accepted industry practices and the wiggle room provided by requiring reasonable but not strict adherence to those practices.[62]

FTC v. Toysmart.com

Civ. Action No. 00-11341-RGS (FTC July 21, 2000),

COMPLAINT

. . . . 4. Defendants Toysmart.com, Inc. and Toysmart.com, LLC (collectively "Toysmart" or "defendant") are Delaware corporations. . . .

6. Since at least January 1999, Toysmart has advertised, promoted, and sold toys on the Internet, located at www.toysmart.com. Toysmart markets its products and services throughout the United States and the world via the Internet.

7. In connection with its Web site, Toysmart collects personal customer information including, but not limited to, consumers' names, addresses, billing information, shopping preferences, and family profile information ("Customer Lists").

8. In September 1999, Toysmart became a licensee of TRUSTe, an organization that certifies the privacy policies of online businesses and allows such businesses to display a TRUSTe trustmark or seal.

9. From September 1999 to the present, the privacy policy posted on the Toysmart.com Web site has stated, *inter alia*, (1) "Personal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party. All information obtained by toysmart.com is used only to personalize your experience online;" and (2) "When you register with toysmart.com, you can rest assured that your information will never be shared with a third party." A true and correct copy of the Toysmart privacy policy is attached hereto as Exhibit 1.

10. On May 22, 2000, Toysmart announced that, as of midnight on May 19, 2000, it had officially ceased operations. Toysmart also announced that it had retained the services of a Boston-based management consultant, The Recovery

[62] Solove & Hartzog, *Scope and Potential of FTC, supra*.

Group, to locate parties interested in acquiring Toysmart.com's business and assets.

11. On May 22, 2000, Toysmart began soliciting bids for the purchase of its assets. Bids have been sought for the purchase of all of the company's assets or for individual assets. Among the individual assets offered for sale by Toysmart.com are its Customer Lists (on either an exclusive or non-exclusive basis). Other assets available include inventory; warehouse fixtures and equipment; intangible assets including domain name, product databases, and Web site source code; and a B2B business plan. Bids were due to Toysmart by 6:00 p.m. EST on June 19, 2000.

12. On June 9, 2000, Toysmart's creditors filed a petition for involuntary bankruptcy. *See In Re: Toysmart.com, LLC*, No. 00-13995-CJK (Bankr. D. Mass).

13. On June 19, 2000, bidding for Toysmart's assets concluded. Toysmart informed the Federal Trade Commission that its Customer Lists will not be transferred to a third party absent bankruptcy court approval. . . .

17. From at least September 1999 to the present, defendant Toysmart, directly or through its employees and agents, in connection with its collection of personal consumer information, expressly and/or by implication, represented that it would "never" disclose, sell, or offer for sale customers' or registered members' personal information to third parties.

18. In truth and in fact, Toysmart has disclosed, sold, or offered for sale its customer lists and profiles. Therefore, the representation set forth in Paragraph 17 was, and is, a deceptive practice. . . .

STIPULATION AND ORDER ESTABLISHING CONDITIONS ON SALE OF CUSTOMER INFORMATION

This Stipulation is entered into this twentieth day of July, 2000, by and between, Toysmart.com, LLC, debtor and debtor-in-possession ("Debtor" or "Toysmart"), and the Federal Trade Commission ("FTC"). . . .

For the purposes of this Agreement, the following definitions shall apply:

"Qualified Buyer" shall mean an entity that (1) concentrates its business in the family commerce market, involving the areas of education, toys, learning, home and/or instruction, including commerce, content, product and services, and (2) expressly agrees to be Toysmart's successor-in-interest as to the Customer Information, and expressly agrees to the obligations set forth in Paragraphs 2, 3 and 4, below. . . .

The Debtor shall only assign or sell its Customer Information as part of the sale of its Goodwill and only to a Qualified Buyer approved by the Bankruptcy Court. In the process of approving any sale of the Customer Information, the Bankruptcy Court shall require that the Qualified Buyer agree to and comply with the terms of this Stipulation.

The Qualified Buyer shall treat Customer Information in accordance with the terms of the Privacy Statement and shall be responsible for any violation by it following the date of purchase. Among other things, the Qualified Buyer shall use Customer Information only to fulfill customer orders and to personalize customers' experience on the Web site, and shall not disclose, sell or transfer Customer Information to any Third Party.

If the Qualified Buyer materially changes the Privacy Statement, prior notice will be posted on the Web site. Any such material change in policy shall apply only to information collected following the change in policy. The Customer Information shall be governed by the Privacy Statement, unless the consumer provides affirmative consent ("opt-in") to the previously collected information being governed by the new policy.

In the event that an order is not entered on or before July 31, 2001, approving the sale of the Customer Information to a Qualified Buyer or approving a plan of reorganization, the Debtor shall, on or before August 31, 2001, delete or destroy all Customer Information in its possession, custody or control, and provide written confirmation to the FTC, sworn to under penalty of perjury, that all such Customer Information has been deleted or destroyed. Pending approval of any sale of the Customer Information to a Qualified Buyer or of a plan of reorganization, the Debtor shall handle Customer Information in accordance with the Privacy Statement.

This Stipulation and Order, after approval by the Bankruptcy Court, shall be attached to and incorporated in full into the terms of any plan of liquidation or reorganization that is ultimately approved in this bankruptcy case.

STATEMENT OF COMMISSIONER MOZELLE W. THOMPSON

. . . I have voted to approve the settlement in this matter resolving the Commission's charges that Toysmart violated Section 5 of the Federal Trade Commission Act because I believe the terms of the settlement are consistent with Toysmart's privacy policy. More specifically, the settlement permits Toysmart to sell its information only to a "qualified buyer," defined as an entity engaged in the family commerce market who *expressly agrees to be Toysmart's successor-in-interest as to that information*. Accordingly, Toysmart may transfer its data only to someone who specifically "stands" in the shoes of Toysmart.

Despite the consistency between the settlement and Toysmart's privacy policy, my decision to approve the settlement is not without reservation. Like my colleagues Commissioner Anthony and Commissioner Swindle, I think that consumers would benefit from notice and choice before a company transfers their information to a corporate successor. Indeed, many of the consumers who disclosed their families' personal information to Toysmart might not have been willing to turn over the same information to the particular corporate entity that ultimately succeeds Toysmart. This is true even where Toysmart's corporate successor must pursue the same line of business as its predecessor.

I urge any successor to provide Toysmart customers with notice and an opportunity to "opt out" as a matter of good will and good business practice. . . .

STATEMENT OF COMMISSIONER SHEILA F. ANTHONY

The settlements attempt to satisfy both the privacy interests of consumers and the business needs of a failing firm by establishing the conditions on the sale of Toysmart's customer list. Specifically, the order proposed to be filed with the bankruptcy court limits to whom Toysmart may sell its customer list. Toysmart

may only sell the customer list in connection with its goodwill, not as a stand-alone asset, and only to a qualified buyer. . . .

To accept the bankruptcy settlement would place business concerns ahead of consumer privacy. Although the proposed settlement's definition of a qualified buyer attempts to ensure that only an entity "similar" to Toysmart is eligible to purchase the list, I do not believe that this limitation is an adequate proxy for consumer privacy interests. In my view, consumer privacy would be better protected by requiring that consumers themselves be given notice and choice before their detailed personal information is shared with or used by another corporate entity — especially where, as here, consumers provided that information pursuant to a promise not to transfer it.

DISSENTING STATEMENT OF COMMISSIONER ORSON SWINDLE

Defendant Toysmart.com, Inc. ("Toysmart") represented that it would never disclose, sell, or offer to sell the personal information of its customers to a third party. When faced with severe financial difficulties, however, Toysmart solicited bids for its customer lists, which include or reflect the personal information of its customers. . . .

I agree that a sale to a third party under the terms of the Bankruptcy Order would be a substantial improvement over the sale that likely would have occurred without Commission action. Nevertheless, I do not think that the Commission should allow the sale. If we really believe that consumers attach great value to the privacy of their personal information and that consumers should be able to limit access to such information through private agreements with businesses, we should compel businesses to honor the promises they make to consumers to gain access to this information. Toysmart promised its customers that their personal information would *never* be sold to a third party, but the Bankruptcy Order in fact would allow a sale to a third party. In my view, such a sale should not be permitted because "never" really means never.

I dissent.

NOTES & QUESTIONS

1. ***Postscript.*** After the FTC approved the settlement in *Toysmart* by a 3-2 vote by the commissioners, the settlement attracted the support of Toysmart's creditors, since it would allow the sale of the database to certain purchasers, and hence could be used to pay back the creditors. However, in August 2000, Judge Carol Kenner of the U.S. Bankruptcy Court rejected the settlement because there were currently no offers on the table to buy the database, and it would hurt the creditors to restrict the sale to certain types of purchasers without first having a potential buyer. In February 2001, Judge Kenner agreed to let Toysmart sell its customer database to Disney, the primary shareholder, for $50,000. Disney agreed, as part of the deal, to destroy the list.

   The Toysmart bankruptcy also led Amazon.com, the Internet's largest retailer, to change its privacy policy. Prior to the Toysmart case, Amazon's privacy policy provided:

> Amazon.com does not sell, trade, or rent your personal information to others. We may choose to do so in the future with trustworthy third parties, but you can tell us not to by sending a blank e-mail message to never@amazon.com.

In its new policy, Amazon.com stated:

> Information about our customers is an important part of our business, and we are not in the business of selling it to others. We share customer information only with the subsidiaries Amazon.com, Inc., controls and as described below. . . .
>
> As we continue to develop our business, we might sell or buy stores or assets. In such transactions, customer information generally is one of the transferred business assets. Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets. . . .

Amazon.com's new policy was criticized by some privacy organizations. One of the criticisms was that the policy did not provide an opt-out right. Suppose Amazon.com went bankrupt and decided to sell all of its customer data. Can it sell data supplied by consumers under the old policy? Can the new policy apply retroactively?

2. ***Bankruptcy: Property Rights vs. Contract Rights.*** Edward Janger proposes that a property rights regime (as opposed to the contractual rights of a privacy policy) will best protect the privacy of personal data when companies possessing such data go bankrupt:

> Property rules are viewed as reflecting undivided entitlements. They allocate, as Carol Rose puts it, the "whole meatball" to the "owner." Liability rules, by contrast are viewed as dividing an entitlement between two parties. One party holds the right, but the other party is given the option to take the right and compensate the right holder for the deprivation (to breach and pay damages). . . .
>
> Propertization has some crucial benefits, but it also has some serious costs. Both the bankruptcy and non-bankruptcy treatment of privacy policies turn on whether a privacy policy creates a right enforceable only through civil damages, or a right with the status of property. If bankruptcy courts treat privacy policies solely as contract obligations [the liability rule], the debtor will be free to breach (or reject) the contract in bankruptcy. Any damage claim will be treated as a prepetition claim, paid, if at all, at a significant discount. Consumer expectations (contractual or otherwise) of privacy are likely to be defeated. By contrast, if personal information is deemed property subject to an encumbrance, then the property interest must be respected, or to use the bankruptcy term, "adequately protected."

In other words, Janger contends that giving individuals property rights in their personal data will provide more protection than giving individuals contract rights in the event a company goes bankrupt.[63]

[63] Edward J. Janger, *Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy*, 44 Wm. & Mary L. Rev. 1801 (2002).

3. ***Customer Databases as Collateral.*** Xuan-Thao Nguyen points out that companies are using their customer databases as collateral for loans, since these databases are one of their most significant assets:

> Whether intentional or unintentional, many Internet companies ignore their own privacy policy statements when the companies pledge their customer database as collateral in secured financing schemes. This practice renders online privacy statements misleading because the statements are silent on collateralization of the company's assets. . . .
>
> The secured party can use the consumer database in its business or sell the consumer database to others. The collateralization of the consumer database and its end result may contradict the debtor's consumer privacy statement declaring that the debtor does not sell or lease the consumer information to others. Though there is no direct sale of the consumer database to the secured party, the effect of the collateralization of the consumer database is the same: the consumer database is in the hands of third parties with unfettered control and rights. Essentially, the collateralization of consumer databases violates the privacy policies publicized on debtors' Web sites.[64]

4. ***Retroactive Changes to Privacy Policies.*** In *In the Matter of Gateway, Inc.*, 2004 WL 261847 (FTC Sept. 10, 2004), Gateway Learning Corp. collected personal information from its consumers pursuant to a privacy policy stating that it would not sell, rent, or loan personal information to third parties unless people consented. It also promised that if it changed its privacy policy, it would give consumers the opportunity to "opt out" of having their data shared.

   Subsequently, Gateway altered its privacy policy to allow the renting of personal information to third parties without informing customers and obtaining their explicit consent. The FTC filed a complaint alleging that this practice was an unfair practice. The FTC also charged that Gateway's failure to inform consumers of its changes to its privacy policies, despite its promises to do so, constituted a deceptive practice. Gateway settled with the FTC, agreeing that it would "not misrepresent . . . [t]he manner in which [it] will collect, use, or disclose personal information." It also agreed to pay $4,608, which was the amount it earned from renting the information.

   Suppose a company puts the following line in its privacy policy: "Please be aware that we may change this policy at any time." Would this allow for the retroactive application of a revised policy? Or is there an argument that even with a statement such as this one, the revised policy could not be applied retroactively?

5. ***Apps with Privacy Policies.*** Increasingly, users of various websites, software, and mobile devices are using applications (called "apps") developed by third parties. These apps add special features and functions and are quite popular. Many app developers are small companies or individuals without the normal cadre of lawyers, privacy officers, and other experts. At the same time, many apps gather a lot of personal information. In 2011, the Future of Privacy Forum (FPF), a privacy think tank, examined the top paid apps for mobile devices (such as the iPhone, Android, and Blackberry). FPF found that 22 out of 30 did not have a privacy policy. Without a privacy policy, would the FTC have theories upon which it could enforce privacy protections against the app? Could the FTC require apps to have privacy policies?

[64] Xuan-Thao N. Nguyen, *Collateralizing Privacy,* 78 Tul. L. Rev. 553, 571, 590 (2004).

IN THE MATTER OF FACEBOOK, INC.

2012 WL 3518628 (FTC July 27, 2012)

COMPLAINT

The Federal Trade Commission, having reason to believe that Facebook, Inc., a corporation ("Respondent") has violated the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges: . . . .

3. Since at least 2004, Facebook has operated www.facebook.com, a social networking website. Users of the site create online profiles, which contain content about them such as their name, interest groups they join, the names of other users who are their "friends" on the site, photos albums and videos they upload, and messages and comments they post or receive from their friends. Users also may add content to other users' profiles by sharing photos, sending messages, or posting comments. As of March 2012, Facebook had approximately 900 million users.

4. Since approximately May 2007, Facebook has operated the Facebook Platform ("Platform"), a set of tools and programming interfaces that enables third parties to develop, run, and operate software applications, such as games, that users can interact with online ("Platform Applications"). . . .

6. Facebook has collected extensive "profile information" about its users, including, but not limited to [name, gender, email address, birthday, profile picture, photos, friends, and other personal data]. . . .

9. Facebook has designed its Platform such that Platform Applications can access user profile information in two main instances. First, Platform Applications that a user authorizes can access the user's profile information. Second, if a user's "Friend" authorizes a Platform Application, that application can access certain of the user's profile information, even if the user has not authorized that Application. For example, if a user authorizes a Platform Application that provides reminders about Friends' birthdays, that application could access, among other things, the birthdays of the user's Friends, even if these Friends never authorized the application.

10. Since at least November 2009, Facebook has, in many instances, provided its users with a "Central Privacy Page," the same or similar to the one depicted below. Among other things, this page has contained a "Profile" link, with accompanying text that has stated "[c]ontrol who can see your profile and personal information."

11. When users have clicked on the "Profile" link, Facebook has directed them to a "Profile Privacy Page," the same or similar to the one depicted below, which has stated that users could "[c]ontrol who can see your profile and related information." For each "Profile Privacy Setting," depicted below, users could click on a drop-down menu and restrict access to specified users, *e.g.*, "Only Friends," or "Friends of Friends."

12. Although the precise language has changed over time, Facebook's Central Privacy Page and Profile Privacy Page have, in many instances, stated that the Profile Privacy Settings allow users to "control who can see" their profile information, by specifying who can access it, *e.g.*, "Only Friends" or "Friends of Friends."

13. Similarly, although the precise interface has changed over time, Facebook's Profile Privacy Settings have continued to specify that users can restrict access to their profile information to the audience the user selects, *e.g.*, "Only Friends," "Friends of Friends." . . .

14. None of the pages described in Paragraphs 10-13 have disclosed that a user's choice to restrict profile information to "Only Friends" or "Friends of Friends" would be ineffective as to certain third parties. Despite this fact, in many instances, Facebook has made profile information that a user chose to restrict to "Only Friends" or "Friends of Friends" accessible to any Platform Applications that the user's Friends have used (hereinafter "Friends' Apps"). Information shared with such Friends' Apps has included, among other things, a user's birthday, hometown, activities, interests, status updates, marital status, education (*e.g.*, schools attended), place of employment, photos, and videos. . . .

19. On approximately November 19, 2009, Facebook changed its privacy policy to designate certain user information as "publicly available" ("PAI"). On approximately December 8, 2009, Facebook began implementing the changes referenced in its new policy ("the December Privacy Changes") to make public in new ways certain information that users previously had provided.

20. Before December 8, 2009, users could, and did, use their Friends' App Settings to restrict Platform Applications' access to their PAI. For example, as of November 2009, approximately 586,241 users had used these settings to "block" Platform Applications that their Friends used from accessing any of their profile information, including their Name, Profile Picture, Gender, Friend List, Pages, and Networks. Following the December Privacy Changes, Facebook users no longer could restrict access to their PAI through these Friends' App Settings, and all prior user choices to do so were overridden. . . .

22. Before December 8, 2009, users could, and did, use their Search Privacy Settings (available through the "Search" link on the Privacy Settings Page. . . .Following the December Privacy Changes, Facebook users could no longer restrict the visibility of their Profile Picture and Pages through these settings, and all prior user choices to do so were overridden.

23. To implement the December Privacy Changes, Facebook required each user to click through a multi-page notice, known as the Privacy Wizard. . . .

24. The Privacy Wizard did not disclose adequately that users no longer could restrict access to their newly-designated PAI via their Profile Privacy Settings, Friends' App Settings, or Search Privacy Settings, or that their existing choices to restrict access to such information via these settings would be overridden. . . .

26. Facebook's designation of PAI caused harm to users, including, but not limited to, threats to their health and safety, and unauthorized revelation of their affiliations. Among other things:

a. certain users were subject to the risk of unwelcome contacts from persons who may have been able to infer their locale, based on the locales of their Friends (*e.g.*, their Friends' Current City information) and of the organizations reflected in their Pages;

b. each user's Pages became visible to anyone who viewed the user's profile, thereby exposing potentially controversial political views or other sensitive information to third parties — such as prospective employers, government organizations, or business competitors — who sought to obtain personal information about the user;

c. each user's Friend List became visible to anyone who viewed the user's profile, thereby exposing potentially sensitive affiliations, that could, in turn, reveal a user's political views, sexual orientation, or business relationships, to third parties — such as prospective employers, government organizations, or business competitors — who sought to obtain personal information about the user; and

d. each user's Profile Photo became visible to anyone who viewed the user's profile, thereby revealing potentially embarrassing or political images to third parties whose access users previously had restricted.

27. As described in Paragraph 23, Facebook has represented, expressly, or by implication, that its December Privacy Changes provided users with "more control" over their information, including by allowing them to preserve their "Old Settings," to protect the privacy of their profile information.

28. As described in Paragraph 24-26, Facebook failed to disclose, or failed to disclose adequately, that, following the December Privacy Changes, users could no longer restrict access to their Name, Profile Picture, Gender, Friend List, Pages, or Networks by using privacy settings previously available to them. Facebook also failed to disclose, or failed to disclose adequately, that the December Privacy Changes overrode existing user privacy settings that restricted access to a user's Name, Profile Picture, Gender, Friend List, Pages, or Networks. These facts would be material to consumers. Therefore, Facebook's failure to adequately disclose these facts, in light of the representation made, constitutes a deceptive act or practice.

29. As described in Paragraphs 19-26, by designating certain user profile information publicly available that previously had been subject to privacy settings, Facebook materially changed its promises that users could keep such information private. Facebook retroactively applied these changes to personal information that it had previously collected from users, without their informed consent, in a manner that has caused or has been likely to cause substantial injury to consumers, was not outweighed by countervailing benefits to consumers or to competition, and was not reasonably avoidable by consumers. This practice constitutes an unfair act or practice. . . .

34. Facebook has displayed advertisements ("ads") from third-parties ("Platform Advertisers") on its web site.

35. Facebook has allowed Platform Advertisers to target their ads ("Platform Ads") by requesting that Facebook display them to users whose profile information reflects certain "targeted traits," including, but not limited to [location, age, sex, birthday, relationship status, likes, and interests, among other things]. . . .

36. Facebook has disseminated or caused to be disseminated numerous statements that it does not share information about its users with advertisers, including:

> a. Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as ... personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are. (Facebook Privacy Policy, November 26, 2008). . . .
>
> d. Still others asked to be opted-out of having their information shared with advertisers. This reflects a common misconception about advertising on Facebook. We don't share your information with advertisers unless you tell us to ([*e.g.,*] to get a sample, hear more, or enter a contest). Any assertion to the contrary is false. Period ... we never provide the advertiser any names or other information about the people who are shown, or even who click on, the ads. (Facebook Blog, http://blog.facebook.com/blog.php, "Responding to Your Feedback," Barry Schnitt, April 5, 2010). . . .

37. Contrary to the statements set forth in Paragraph 36(a)-(d), in many instances, Facebook has shared information about users with Platform Advertisers by identifying to them the users who clicked on their ads and to whom those ads were targeted. . . .

38. As a result of the conduct described in Paragraph 37, Platform Advertisers potentially could take steps to get detailed information about individual users. . . .

50. As described above, Facebook has collected and stored vast quantities of photos and videos that its users upload, including, but not limited to: at least one such photo from approximately ninety-nine percent of its users, and more than 100 million photos and 415,000 videos from its users, collectively, every day.

51. Facebook has stored users' photos and videos such that each one is assigned a Content URL — a uniform resource locator that specifies its location on Facebook's servers. Facebook users and Platform Applications can obtain the Content URL for any photo or video that they view on Facebook's web site by, for example, right-clicking on it. If a user or Application further disseminates this URL, Facebook will "serve" the user's photo or video to anyone who clicks on the URL.

52. Facebook has disseminated or caused to be disseminated statements communicating that a user can restrict access to his or her profile information — including, but not limited to, photos and videos that a user uploads — by deleting or deactivating his or her user account. Such statements include:

> a. Deactivating or deleting your account. If you want to stop using your account you may deactivate it or delete it. When you deactivate an account, no user will be able to see it, but it will not be deleted. . . . When you delete an account, it is permanently deleted from Facebook. . . .
>
> Backup copies. Removed and deleted information may persist in backup copies for up to 90 days, but will not be available to others; (Facebook Privacy Policy, November 19, 2009). . . .

53. Contrary to the statements set forth in Paragraph 52, Facebook has continued to display users' photos and videos to anyone who accesses Facebook's Content URLs for them, even after such users have deleted or deactivated their accounts. . . .

NOTES & QUESTIONS

1. ***Postscript.*** Facebook settled with the FTC, agreeing to refrain from misrepresenting the privacy of consumer personal data, obtain consent before changing consumer privacy preferences, and establish a comprehensive privacy program, among other things.
2. ***Statements Beyond the Privacy Policy.*** In *Facebook,* the FTC cites statements made in blog posts by Facebook employees when listing various false or misleading claims made by Facebook. When should statements by a company's employees count as official statements of the company? Suppose a company allows employees to have blogs hosted by the company and each blog does not contain any language that indicates that employees are speaking for themselves only. Should statements the employees write on these blogs be considered promises made by the company?

   How specific do statements need to be? In an interview, Mark Zuckerberg assured Facebook users that "[p]rivacy is very important to us."[65] Could vague or broad statements like this one be used by the FTC against Facebook?

   Consider Solove and Hartzog:

   > These cases have made it clear that the question of what constitutes a deceptive trade practice is holistic. Not only does the FTC consider representations beyond what exists in a privacy policy, but it considers consumer expectations as well. This raises a number of interesting questions. The first is the extent to which other representations can contradict explicit representations in the privacy policy. While contract law tends to give great weight to the boilerplate terms of a contract, the FTC does not appear to recognize any kind of significant presumption to exculpatory representations buried in dense legalese that run contrary to other representations or consumer expectations. . . .
   >
   > Finally, given the universe of potential privacy-related statements the FTC could have (and has) drawn from to find deception, has there been a shift from explicit, insular representations to larger framing effects that create consumer trust? In other words, it appears that what a company has promised is simply one factor in a larger approach to determining whether a company has been deceptive. The FTC looks at architecture, shared norms, and cultural assumptions likely held by consumers to determine consumer expectations. This framework developed by the FTC logically would also consider any statement made by the company that would materially contribute to the creation of trust on the part of the consumer.[66]

3. ***Website Design Elements.*** Woodrow Hartzog argues that the privacy expectations of many users of websites is formed not by the privacy policy but by the various privacy settings and design elements of the site.[67] Websites such

[65] John Paczkowski, *Facebook CEO Mark Zuckerberg in the Privacy Hot Seat*, All Things D (June 2, 2010), http://allthingsd.com/20100602/mark-zuckerberg-session/.

[66] Solove & Hartzog, *FTC and the New Common Law of Privacy, supra.*

[67] Woodrow Hartzog, *Website Design as Contract,* 60 Am. U. L. Rev. 1635 (2011).

as Facebook have multiple privacy settings on a page distinct from the privacy policy or terms of use. More people might interact with the privacy settings page than read the privacy policy page.

Suppose certain forms of data sharing are disclosed in the privacy policy but not on the privacy settings page. These forms of data sharing exist no matter what a person's settings are. A user might argue that she did not expect this data sharing because based on the privacy settings page, it appeared as though all her data would only be shared per the settings she set. On the settings page, the company has the following statement, with a link to the privacy policy page: "Please refer to our privacy policy for information about how we collect, use, and share your data." Is this sufficient?

4. ***Is Touting a Service as "Free" a Deceptive Trade Practice?*** Recall Chris Hoofnagle and Jan Whittington's argument that many online services that are purportedly "free" actually have a cost because they gather personal data about consumers and sell this data to advertisers.[68] The FTC, however, has allowed free offers that require a purchase. As Hoofnagle and Whittington describe the FTC's approach:

> [T]he FTC will generally consider the use of free offers to be unfair and deceptive unless two conditions are met. First, the conditions and obligations accompanying the free offer must be set forth at the outset, "so as to leave no reasonable probability that the terms of the advertisement or offer might be misunderstood." Second, sellers cannot offset the cost of providing a free product by increasing the ordinary price, quality, or size of the product that must be purchased in order to obtain the free offer.

According to Hoofnagle and Whittington, under the guidance of the 1971 FTC Guide and subsequent decisions, "sites such as Facebook.com [can] continue to use the term 'free' even when offers are contingent on the consumer's performance of certain obligations, so long as Facebook clearly discloses those obligations." Hoofnagle and Whittington suggest that the FTC should change its approach and take measures to help consumers realize the true nature of online services. For example, they suggest that the FTC could mandate "notice at the time the transaction occurs that the consumer's personal information is the basis of the bargain and that such information may be used for tracking or other secondary purposes." Another solution might be to require free services to offer a paid alternative where personal data would not be used.

[68] Chris Jay Hoofnagle and Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. Rev. 606 (2014).

IN THE MATTER OF SEARS HOLDINGS MANAGEMENT CORP.

2009 WL 2979770 (FTC Aug. 31, 2009)

COMPLAINT

The Federal Trade Commission, having reason to believe that Sears Holdings Management Corporation, a corporation, has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Sears Holdings Management Corporation ("respondent" or "SHMC") is a Delaware corporation with its principal office or place of business at 3333 Beverly Road, Hoffman Estates, Illinois 60179. SHMC, a subsidiary of Sears Holdings Corporation ("SHC") with shares owned by Sears, Roebuck and Co. and Kmart Management Corporation, handles marketing operations for the Sears Roebuck and Kmart retail stores, and operates the sears.com and kmart.com retail Internet websites. . . .

3. From on or about April 2007 through on or about January 2008, SHMC disseminated or caused to be disseminated via the Internet a software application for consumers to download and install onto their computers (the "Application"). The Application was created, developed, and managed for respondent by a third party in connection with SHMC's "My SHC Community" market research program.

4. The Application, when installed, runs in the background at all times on consumers' computers and transmits tracked information, including nearly all of the Internet behavior that occurs on those computers, to servers maintained on behalf of respondent. Information collected and transmitted includes: web browsing, filling shopping baskets, transacting business during secure sessions, completing online application forms, checking online accounts, and, through select header information, use of web-based email and instant messaging services.

5. SHMC, during the relevant time period, presented fifteen out of every hundred visitors to the sears.com and kmart.com websites with a "My SHC Community" pop-up box that said:

> Ever wish you could talk directly to a retailer? Tell them about the products, services and offers that would really be right for you?
>
> If you're interested in becoming part of something new, something different, we'd like to invite you to become a member of My SHC Community. My SHC Community, sponsored by Sears Holdings Corporation, is a dynamic and highly interactive on-line community. It's a place where your voice is heard and your opinion matters, and what you want and need counts!

The pop-up box made no mention of the Application. Likewise, the general "Privacy Policy" statement accessed via the hyperlink in the pop-up box did not mention the Application.

6. The pop-up box message further invited consumers to enter their email address to receive a follow-up email from SHMC with more information. Subsequently, invitation messages were emailed to those consumers who supplied their email address. These emails stated, in pertinent part:

From shopping, current events, social networking, to entertainment and email, it seems that the Internet is playing a bigger and bigger role in our daily lives these days.

If you're interested in becoming part of something new, something different, we'd like to invite you to join a new and exciting online community; My SHC Community, sponsored by Sears Holdings Corporation. *Membership is absolutely free!*

My SHC Community is a dynamic and highly interactive online community. It's a place where your voice is heard and your opinion matters, and what you want and need counts! As a member of My SHC Community, you'll partner directly with the retail industry. You'll participate in exciting, engaging and on-going interactions — always on your terms and always by your choice. My SHC Community gives you the chance to help shape the future by sharing and receiving information about the products, services and offers that would really be right for you.

To become a member of My SHC Community, we simply ask you to complete the registration process which includes providing us with your contact information as well as answering a series of profile questions that will help us get to know you better. You'll also be asked to take a few minutes to download software that is powered by (VoiceFive). This research software will confidentially track your online browsing. This will help us better understand you and your needs, enabling us to create more relevant future offerings for you, other community members, and eventually all shoppers. You can uninstall the software at any time through the Add/Remove program utility on your computer. During the registration process, you'll learn more about this application software and you'll always have the opportunity to ask any and every question you may have.

Once you're a member of My SHC Community, you'll regularly interact with My SHC Community members as well as employees of Sears Holdings Corporation through special online engagements, surveys, chats and other fun and informative online techniques. We'll ask you to journal your shopping and purchasing behavior. Again, this will be when you want and how you want to record it — always on your terms and always by your choice. We'll also collect information on your internet usage. Community engagements are always fun and always voluntary!

The email invitation message then described what consumers would receive in exchange for becoming a member of the My SHC Community, including a $10 payment for joining the "online community," contingent upon the consumer retaining the Application on his or her computer for at least one month. Consumers who wished to proceed further would need to click a button, at the bottom, center portion of the invitation email, that said "Join Today!"

7. Consumers who clicked on the "Join Today!" button in the email invitation were directed to a landing page that restated many of the aforementioned representations about the potential interactions between members and the "community" and about the putative benefits of membership. The landing page did not mention the Application.

8. Consumers who clicked on the "Join Today" button in the landing page were directed to a registration page. To complete registration, consumers needed to enter information, including their name, address, age, and email address. Below the fields for entering information, the registration page presented a "Privacy Statement and User License Agreement" ("PSULA") in a "scroll box" that

displayed ten lines of the multi-page document at a time. A description of the Application's specific functions begins on approximately the 75 line down in the scroll box:

> Computer hardware, software, and other configuration information: Our application may collect certain basic hardware, software, computer configuration and application usage information about the computer on which you install our application, including such data as the speed of the computer processor, its memory capacities and Internet connection speed. In addition, our application may report on devices connected to your computer, such as the type of printer or router you may be using.
>
> Internet usage information: Once you install our application, it monitors all of the Internet behavior that occurs on the computer on which you install the application, including both your normal web browsing and the activity that you undertake during secure sessions, such as filling a shopping basket, completing an application form or checking your online accounts, which may include personal financial or health information. We may use the information that we monitor, such as name and address, for the purpose of better understanding your household demographics; however, we make commercially viable efforts to automatically filter confidential personally identifiable information such as UserID, password, credit card numbers, and account numbers. Inadvertently, we may collect such information about our panelists; and when this happens, we make commercially viable efforts to purge our database of such information.
>
> The software application also tracks the pace and style with which you enter information online (for example, whether you click on links, type in webpage names, or use shortcut keys), the usage of cookies, and statistics about your use of online applications (for example, it may observe that during a given period of use of a computer, the computer downloaded X number of bytes of data using a particular Internet enabled gaming application).
>
> Please note: Our application does not examine the text of your instant messages or e-mail messages. We may, however, review select e-mail header information from web-based e-mails as a way to verify your contact information and online usage information.

The PSULA went on to describe how the information the Application would collect was transmitted to respondent's servers, how it might be used, and how it was maintained. It also described how consumers could stop participating in the online community and remove the Application from their computers. Respondent stated in the PSULA that it reserved the right to continue to use information collected prior to a consumer's "resignation."

9. Below the scroll box on the registration page was a link that consumers could click to access a printable version of the PSULA, and a blank checkbox next to the statement: "I am the authorized user of this computer and I have read, agree to, and have obtained the agreement of all computer users to the terms and conditions of the Privacy Statement and User License Agreement." To continue with the registration process, consumers needed to check the box and click the "Next" button at the bottom of the registration page.

10. Consumers who completed the required information, checked the box, and clicked the "Next" button on the registration page, were directed to an installation page that explained the Application download and installation process. Consumers were required to click a "Next" button to begin the download, and then click an

"Install" or "Yes" button in a "security warning" dialog box to install the Application. Nothing on the installation page provided information on the Application.

11. When installed, the Application functioned and transmitted information substantially as described in the PSULA. The Application, when installed, would run in the background at all times on consumers' computers. Although the Application would be listed (as "mySHC Community") in the "All Programs" menu and "Add/Remove" utilities of those computers, and the Application's executable file name ("srhc.exe") would be listed as a running process in Windows Task Manager, the Application would display to users of those computers no visible indication, such as a desktop or system tray icon, that it was running.

12. The Application transmitted, in real time, tracked information to servers maintained on behalf of respondent. The tracked information included not only information about websites consumers visited and links that they clicked, but also the text of secure pages, such as online banking statements, video rental transactions, library borrowing histories, online drug prescription records, and select header fields that could show the sender, recipient, subject, and size of web-based email messages.

13. Through the means described in paragraphs 3-12, respondent has represented, expressly or by implication, that the Application would track consumers' "online browsing." Respondent failed to disclose adequately that the software application, when installed, would: monitor nearly all of the Internet behavior that occurs on consumers' computers, including information exchanged between consumers and websites other than those owned, operated, or affiliated with respondent, information provided in secure sessions when interacting with third-party websites, shopping carts, and online accounts, and headers of web-based email; track certain non-Internet-related activities taking place on those computers; and transmit nearly all of the monitored information (excluding selected categories of filtered information) to respondent's remote computer servers. These facts would be material to consumers in deciding to install the software. Respondent's failure to disclose these facts, in light of the representations made, was, and is, a deceptive practice.

14. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act. . . .

NOTES & QUESTIONS

1. ***Adequate Notice.*** Sears did disclose how the application worked, though it was buried in a lengthy statement. How prominently must something be mentioned for notice to be adequate? One factor in this case involved the highly invasive functions of the application. Perhaps the prominence of notice should be proportionate to the invasiveness to privacy. But who decides? If many people do not read privacy notices at all, does it matter if a statement appears in line 5 or line 75?
2. ***From Broken Promises to Broken Expectations?*** Solove and Hartzog contend that the FTC has begun to focus away from the explicit promises a company makes and towards ways in which consumer expectations are being thwarted:

> Although the FTC began enforcing broken *promises* of privacy, its focus seems to have shifted to broken *expectations* of consumer privacy. The shift might seem subtle, but it is dramatic in effect. Instead of the core question being what was promised, which largely focuses on a company's language, the core question has become what was expected, which incorporates the universe of preexisting consumer backgrounds, norms, and dispositions, as well as elements of design, functionality, and other nonlinguistic factors besides privacy-related statements that shape a consumer's expectations.
>
> The FTC could simply look at what a company's polices and design/architecture are and compare that with the company's actions. But it is not doing that. Instead, it seems to be taking consumers as it finds them, full of preexisting expectations, contextual norms, and cognitive limitations, and prohibiting companies from exploiting these assumptions and rational ignorance. . . .
>
> If the FTC takes into account the growing evidence about how consumers form their expectations, then it could increasingly demand that companies engage in practices that will correct mistaken consumer assumptions, or at the very least not exploit such assumptions. Existing forms of notice might not be deemed sufficient because the empirical evidence shows that consumers are not really being notified.[69]

3. ***Constructive Sharing of Personally Identifiable Information.*** *In the Matter of MySpace, LLC* (FTC 2012) involved the "constructive sharing" of non-personally identifiable information (PII) — sharing non-PII with third parties that can be used by third parties to access PII. The FTC alleged that MySpace shared non-PII in this manner without indicating to users that the non-PII could be used by third parties to obtain PII. Hence, MySpace's statement that it does not share PII with third parties was misleading.
4. ***Violating the Privacy Policies of Others.*** Most FTC enforcement actions against companies are for violating their own privacy policies. What if a company violates the privacy policy of another company? In In re Vision I Properties (FTC 2005), Vision I Properties licensed shopping cart software and provided related services to small online retail merchants. The company's software created customizable shopping cart pages for client merchants' websites. The resulting pages resided on websites managed by Vision I Properties, but resembled the other pages on its client merchants' websites. Vision I Properties violated the privacy promises of some of these client merchants as stated in their websites; it rented consumers' personal information collected through its shopping cart software. This personal information was then used by third parties to send direct mail and make telemarketing calls to consumers. For the FTC, it was reasonable for consumers to rely on merchants' privacy policies. Moreover, Vision I Properties did not adequately inform merchants of its information sharing. Vision I settled, agreeing to cease selling the data, to provide better notice and to disgorge $9,101 of profits.

---

[69] Solove & Hartzog, *FTC and the New Common Law of Privacy, supra.*

5. ***Duties When Contracting with Data Service Providers.*** *In the Matter of GMR Transcription Services, Inc.* (FTC 2014) concerned the inadvertent disclosure of medical data by a data service provider hired by GMR, a company that provides medical transcription services. The FTC faulted GMR for its data service provider management practices. According to the FTC complaint, GMR failed to "adequately verify that their service provider, Fedtrans, implemented reasonable and appropriate security measures to protect personal information in audio and transcript files on Fedtrans' network and computers used by Fedtrans' typists."

   Moreover, the FTC faulted GMR for failures in contracting with its data service provider. The FTC complaint alleged that GMR failed to "require Fedtrans by contract to adopt and implement appropriate security measures to protect personal information in medical audio and transcript files, such as by requiring that files be securely stored and securely transmitted to typists (e.g., through encryption) and authenticating typists (e.g., through unique user credentials) before granting them access to such files; take adequate measures to monitor and assess whether Fedtrans employed measures to appropriately protect personal information under the circumstances."

   The FTC additionally found GMR to be deficient in doing due diligence before hiring its data service provider: "Respondents did not request or review relevant information about Fedtrans' security practices, such as, for example, Fedtrans' written information security program or audits or assessments Fedtrans may have had of its computer network."

   Looking broadly at the complaint, there are three things that the FTC requires companies to do when contracting with data service providers: (1) exercise due diligence before hiring these third parties; (2) have appropriate protections of data in their contracts with data service providers; and (3) take steps to verify that the data service providers are adequately protecting data.

6. ***State Deceptive Trade Practices Acts.*** In addition to the FTC Act, which is enforced exclusively by the FTC, every state has some form of deceptive trade practices act of its own. Many of these statutes not only enable a state attorney general to bring actions but also provide a private cause of action to consumers. Several of these laws have provisions for statutory minimum damages, punitive damages, and attorneys' fees. *See, e.g.,* Cal. Civ. Code § 1780(a)(4) (punitive damages); Conn. Gen. Stat. § 42-110g(a) (punitive damages); N.Y. Gen. Bus. Law § 349(h) (minimum damages). In interpreting these state laws, many state courts have been heavily influenced by FTC Act jurisprudence. However, as Jeff Sovern notes, many states "have been more generous to consumers than has the FTC," and "even if the FTC concludes that practices pass muster under the FTC Act, it is still at least theoretically possible for a state to find the practices deceptive under their own legislation." Thus, Sovern concludes, "information practices that are currently in widespread use may indeed violate state little FTC Acts. Marketers should think carefully about whether they wish to alter their practices."[70]

[70] Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 Fordham L. Rev. 1305, 1352-53, 1357 (2001).

IN THE MATTER OF NOMI TECHNOLOGIES, INC.

2015 WL 5304114 (FTC Aug. 28, 2015)

COMPLAINT

3. Nomi uses mobile device tracking technology to provide analytics services to brick and mortar retailers through its "Listen" service. . . .

4. Nomi places sensors in its clients' retail locations that detect the media access control ("MAC") address broadcast by a mobile device when it searches for WiFi networks. A MAC address is a 12-digit identifier that is unique to a particular device. Alternatively, in some instances Nomi collects MAC addresses through its clients' existing WiFi access points. . . .

7. Nomi uses the information it collects to provide analytics reports to its clients about aggregate customer traffic patterns. . . .

10. Nomi does not require its clients to post disclosures or otherwise notify consumers that they use the Listen service. Through October 22, 2013, most, if not all, of Nomi's clients did not post any disclosure, or otherwise notify consumers, regarding their use of the Listen service.

11. Nomi provided, and continues to provide, an opt out on its website for consumers who do not want Nomi to store observations of their mobile device. Once a consumer has entered the MAC address of their device into Nomi's website opt out, Nomi adds it to a blacklist of MAC addresses for which information will not be stored. Nomi did not make an opt out available through any other means, including at any of its clients' retail locations.

12. From at least November 2012, until October 22, 2013, Nomi disseminated or caused to be disseminated privacy policies on its website, nomi.com or getnomi.com, which included the following statement:

> Nomi pledges to .... Always allow consumers to opt out of Nomi's service on its website as well as at any retailer using Nomi's technology. (*See* Exhibits A-C).

13. In order to opt out of the Listen service on Nomi's website, consumers were required to provide Nomi with all of their mobile devices' MAC addresses, without knowing whether they would ever shop at a retail location using the Listen service. Consumers who did not opt out on Nomi's website and instead wanted to make the opt out decision at retail locations were unable to do so, despite the explicit promise in Nomi's privacy policies. Consumers were not provided any means to opt out at retail locations and were unaware that the service was even being used.

VIOLATIONS OF THE FTC ACT

14. As described in Paragraph 12, Nomi represented, directly or indirectly, expressly or by implication, that consumers could opt out of Nomi's Listen service at retail locations using this service.

15. In fact, Nomi did not provide an opt-out mechanism at its clients' retail locations. Therefore, the representation set forth in Paragraph 14 is false or misleading.

16. As described in Paragraph 12, Nomi represented, directly or indirectly, expressly or by implication, that consumers would be given notice when a retail location was utilizing Nomi's Listen service.

17. In fact, neither Nomi nor its clients disclosed to consumers that Nomi's Listen service was being used at a retail location. Therefore, the representation set forth in Paragraph 16 is false or misleading.

18. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act. . . .

DISSENTING STATEMENT OF COMMISSIONER MAUREEN K. OHLHAUSEN

On April 23, 2015, a divided Commission issued a complaint and accepted a proposed consent order with regard to the practices of Nomi Technologies, Inc., a startup company offering its retail merchant clients the ability to analyze aggregate data about consumer traffic in the merchants' stores. . . .

The record now before the Commission confirms that the FTC should not have adopted this complaint and order because it undermines the Commission's own goals of increased consumer choice and transparency of privacy practices and because the order imposes a penalty far out of proportion to the non-existent consumer harm.

The FTC has long called on companies to implement best practices "giving consumers greater control over the collection and use of their personal data through simplified choices and increased transparency."[4] Consistent with such best practices, Nomi went beyond its legal duty by offering increased transparency and consumer choice through an easy and effective global opt-out. Granted, part of Nomi's privacy policy was inaccurate because the company promised, but failed to implement, an additional privacy choice for consumers. However, by applying a *de facto* strict liability deception standard absent any evidence of consumer harm, the proposed complaint and order inappropriately punishes a company that acted consistently with the FTC's privacy goals by offering more transparency and choice than legally required.

The record demonstrates that this enforcement action may, ironically, undermine the FTC's own established privacy goals. Commenters generally agree that the order will diminish companies' incentives to be transparent about their privacy practices. . . .

I share one commenter's particular concern that "the takeaway for most companies will be: if you do not want the FTC to come after you, do the bare-minimum on privacy." . . . Another pointed out that "[t]he ironic upshot of the majority decision is that Nomi could have avoided the FTC enforcement action altogether by not posting a privacy policy, not describing its practices to consumers, and not offering an opt-out mechanism at all."[11] Indeed, upon learning of the Commission's investigation, Nomi simply eliminated a potential privacy choice from its privacy policy. . . .

I conclude that the comments on the record and the marketplace reaction to the complaint and order provide additional persuasive evidence that the costs of this enforcement action outweigh the benefits. The Commission therefore ought to vacate the proposed complaint and consent order. Because the majority declines to do so, I dissent.

DISSENTING STATEMENT OF COMMISSIONER JOSHUA WRIGHT

Nomi does *not* track individual consumers—that is, Nomi's technology records whether individuals are unique or repeat visitors, but it does not identify them. Nomi provides analytics services based upon data collected from mobile device tracking technology to brick-and-mortar retailers through its "Listen" service. …

The Commission's complain focuses upon a single statement in Nomi's privacy policy. Specifically, Nomi's privacy policy states that "Nomi pledges to … Always allow consumers to opt out of Nomi's service on its websites as well as at any retailer using Nomi's technology." …

The fundamental failure of the Commission's complaint is that the evidence simply does not support the allegation that Nomi's representation about an opportunity to opt out of the Listen service at the retail level – in light of the immediate and easily accessible opt out available on the webpage itself – was material to consumers. This failure alone is fatal. … Deception causes consumer harm because it influences consumer behavior – that is, the deceptive statement is one that is not merely misleading in the abstract but one that causes consumers to make choices to their detriment that they would not have otherwise made.

STATEMENT OF COMMISSIONER JULIE BRILL

I vote to finalize the Nomi case, for the reasons articulated in the Majority Statement.

In her dissent, Commissioner Ohlhausen expresses concern that our order will deter companies from offering privacy choices in the marketplace. I agree that, in approving our orders, we should always consider whether they provide the appropriate marketplace incentives. I believe this order provides companies with an incentive to periodically review the statements they make to consumers, and make sure their practices line up with those statements. In this case, we took issue with the fact that Nomi offered a deceptive choice to consumers for nearly a year. Our order today makes sure that this doesn't happen again. In addition, the concern that our order will deter companies from offering choices is belied by the fact that, like many of its competitors in retail mobile location tracking, Nomi continues to offer an online choice to consumers to opt-out of retail mobile tracking. However, as a result of our order, the company no longer offers a deceptive choice.

NOTES & QUESTIONS

1. ***Penalized for Providing Privacy Beyond Legal Requirements?*** Commissioner Ohlhausen argues that the FTC action against Nomi penalizes it for offering opt out rights to individuals when it is not forced to do so. She notes that Nomi could simply have not made such a promise to individuals. Commissioner Brill implies that Nomi's decision to offer choices to consumers might be a

competitive business decision. Whom do you think has the better argument? If companies are not held accountable for their promises to provide privacy choices or protections beyond the minimum required, then would people trust such promises? Should it matter whether or not privacy promises are being made by a company to obtain a competitive advantage?

F. STATUTORY REGULATION

Numerous statutes are directly and potentially applicable to the collection, use, and transfer of personal information by commercial entities. Congress's approach is best described as "sectoral," as each statute is narrowly tailored to particular types of businesses and services. The opposite of sectoral in this context is omnibus, and the United States lacks such a comprehensive statute regulating the private sector's collection and use of personal information. Such omnibus statutes are standard in much of the rest of the world. All member nations of the European Union have enacted omnibus information privacy laws.

In the United States, sectoral laws also do not regulate all commercial entities in their collection and use of personal information. Thus far, federal statutes regulate three basic areas: (a) entertainment records (video and cable television); (b) Internet use and electronic communications; and (c) marketing (telemarketing and spam). As you examine the existing statutes, think about the kinds of commercial entities that the law does not currently regulate. Consider whether these entities should be regulated. Also consider whether one omnibus privacy law can adequately apply to all commercial entities. Would the differences between types of commercial entities make a one-size-fits-all privacy law impractical?

The sectoral statutes embody the Fair Information Practices originally developed by HEW and incorporated into the Privacy Act. However, not all statutes embody all of the Fair Information Practices. As you study each statute, examine which of the Fair Information Practices are required by each statute and which are not.

1. ENTERTAINMENT RECORDS

(a) The Video Privacy Protection Act

Incensed when a reporter obtained a list of videos that Supreme Court Justice Nominee Robert Bork and his family had rented from a video store, Congress passed the Video Privacy Protection Act (VPPA) of 1988, Pub. L. No. 100-618. The VPPA is also known as the "Bork Bill."

Scope. The VPPA is written in technology-neutral terms. It defines a "video tape service provider" as "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 visual materials. . . ." § 2710(a)(4). This statutory language allows the VPPA to extend to DVDs (as opposed to video cassette tapes) and also covers online delivery of movies and other content.

Opt in for Disclosure. The VPPA prohibits videotape service providers from knowingly disclosing personal information, such as titles of videocassettes rented or purchased, without the individual's written consent.

Online providers of video content lobbied Congress, contending that VPPA's opt-in requirement prevented them from integrating into Facebook. They complained that VPPA required consent before each instance where video preferences were shared on social networks. They wanted a single consent to the practice of displaying video "likes" rather than a requirement of consent for each video.

In 2012, Congress passed the Video Privacy Protection Act Amendments Act, which was signed into law in early 2013. These amendments make it easier to obtain consent. Now, consumers can consent via electronic means. Additionally, consent can be obtained in advance for a period of two years. People can later withdraw consent if they choose. A videotape service provider must provide an opportunity "in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election."

Exceptions Allowing Disclosure Without Consent. The VPPA contains several exceptions, permitting videotape providers to disclose "to any person if the disclosure is incident to the ordinary course of business of the video tape service provider." § 2710(b)(2)(E).

The statute provides that "the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer." § 2710(b)(2)(D)(ii). Videotape service providers can disclose the names and addresses of consumers if the consumer has been given the right to opt out, and the disclosure does not identify information about the videos the consumer rents. § 2710(b)(2)(D).

The statute also permits disclosure to the consumer, § 2710(b)(2)(A); disclosure with the informed written consent of the consumer, § 2710(b)(2)(B); disclosure to a law enforcement agency pursuant to a warrant or subpoena, § 2710(b)(2)(C); and disclosure for civil discovery if there is notice and an opportunity to object, § 2710(b)(2).

Destruction of Records. The VPPA requires that records of personal information be destroyed as soon as practicable. § 2710(e).

Preemption. The VPPA does not block states from enacting statutes that are more protective of privacy. § 2710(f).

Enforcement. The VPPA creates a private cause of action when a videotape service provider "knowingly discloses . . . personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1). The VPPA permits recovery of actual damages and provides for liquidated damages in the amount of $2,500. The Act also authorizes recovery for punitive damages, attorneys' fees, and enables equitable and injunctive relief. § 2710(c). The VPPA also includes a statutory exclusionary rule that prevents the admission into evidence of any information obtained in violation of the statute. § 2710(d).

VPPA damages are only available for unauthorized disclosures, not failure to meet other requirements of the act such as the destruction of records. In *Sterk v. Redbox Automated Retail LLC,* 672 F.3d 535 (2012), the court rejected a plaintiff's lawsuit for failure to destroy plaintiff's records in a timely manner, concluding that "[u]nlawful disclosure is the only misconduct listed in the statute for which an award of damages is an appropriate remedy."

NOTES & QUESTIONS

1. ***Netflix and Frictionless Sharing.*** William McGeveran criticizes the Video Privacy Protection Act Amendments Act, which permits Netflix and other online video service providers to obtain a broad ongoing consent from consumers to display the videos they like on Facebook and other social media sites. According to McGeveran, the former VPPA requirement that users must provide consent for each and every disclosure of videos they watch created a type of "friction" on sharing information. The change to VPPA makes sharing videos more "frictionless."[71] McGeveran warns that frictionless sharing interfaces can be "badly designed" leading to misdisclosures and a lack of clear notice to consumers. People can readily forget that their actions are being broadcast and might end up disclosing things they did not want to disclose. McGeveran suggests that friction can be a good thing and should not be removed entirely from sharing. He suggests one way that friction could be added:

   > Netflix could simply put a "PLAY AND SHARE" button next to the "PLAY" button that viewers already must click to stream any video. An interface would not satisfy this law of friction if it required more effort for customers to start viewing a movie than to inform all their Facebook friends what they are watching.

   To what extent should the law mandate that friction be included in the design of online sharing technologies?
2. ***Private Right of Action vs. Agency Enforcement.*** The VPPA is enforced by a private right of action. Other privacy laws are enforced by agencies, such as HIPAA which is enforced by HHS and COPPA which is enforced by the FTC. Should VPPA have been written to not include a private right of action and be enforced by the FTC instead? Is a private right of action a better or worse method of enforcement than agency enforcement? If the answer depends upon specific contexts and types of data, what factors should be considered in evaluating the desirability of having a private right of action?
3. ***The Narrow Focus of VPPA.*** The VPPA was passed in reaction to an attempt to obtain data on what videos Judge Bork watched. The law has been criticized for being too specifically focused on videos and ignoring other forms of media, such as books, magazines, and music. Should VPPA be expanded to cover such things? What about the Internet sites one visits? Or other merchandise one buys, including food, furniture, cars, etc.? Is there a reasonable limiting principle that would limit such an expanded law's scope?

[71] William McGeveran, *The Law of Friction*, 2013 U. Chi. Legal F. 15, 18.

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 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.

NOTES & QUESTIONS

1. ***To Whom Does VPPA Apply?*** The key question in *Dirkes* and *Daniel* is whether the VPPA *only* regulates videotape service providers. The *Daniel* court answered this question affirmatively; the *Dirkes* court 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?
2. ***Facebook, Beacon, Blockbuster, and a VPPA Violation?*** In April 2008, Cathryn Elain Harris filed a lawsuit against Blockbuster Video (a video tape service provider) and Facebook claiming violations of the VPPA. The complaint objected to Blockbuster reporting its customers' activities to Facebook through the Beacon program.

   Facebook introduced Beacon in November 2007; under it, partner companies shared information with Facebook about Facebook user activity that took place on their websites. Initially, this information became part of one's Facebook profile unless the user opted out. After consumer protest, Facebook changed its policy to require that a Facebook user would have to opt in to Beacon before information was disclosed on her Facebook page. It is not clear, however, whether opting out of Beacon stops partner companies from sharing information with Facebook.

   The Harris complaint alleges that Blockbuster's website is still reporting a user's activities back to Facebook, whether or not the consumer opts out of having the information associated with her Facebook profile. Does the Blockbuster-Beacon-Facebook behavior, if as alleged, violate the VPPA? If so, what measure of damages should be used?

IN RE HULU PRIVACY LITIGATION

2012 WL 3282960 (N.D. Cal. 2012)

BEELER, MAGISTRATE J. . . . In this putative class action, viewers of Hulu's on-line video content allege that Hulu wrongfully disclosed their video viewing selections and personal identification information to third parties such as online ad networks, metrics companies (meaning, companies that track data), and social networks, in violation of the Video Privacy Protection Act, 18 U.S.C. § 2710. . . .

Defendant Hulu moves to dismiss the claim under Federal Rule of Civil Procedure 12(b)(1). . . .

Hulu operates a website called Hulu.com that provides video content, both previously released and posted and originally developed. . . .

Plaintiffs and Class Members used their Internet-connected computers and browsers to visit hulu.com and view video content. They were renters, purchasers, and/or subscribers of goods and/or services from Hulu and so were consumers as defined in the Video Privacy Protection Act. . . .

Plaintiffs value their privacy while web-browsing; they do not want to be tracked online; their web browsing (including their viewing choices) involves personal information that is private. . . .

Hulu allowed a metrics company called KISSmetrics to place code containing tracking identifiers on Plaintiffs' computers in the browser cache, Adobe Flash local storage, or DOM local storage. This code allegedly "respawned" or "resurrected" previously-deleted cookies. This code was "inescapable" and allowed Plaintiffs' data to be "retained ... so that they could be tracked over long periods of time and across multiple websites, regardless of whether they were registered and logged in." As a result, when Class Members viewed video content on Hulu.com, Hulu transmitted their video viewing choices and personally identifiable information to third parties without obtaining their written consent before the disclosure. The third parties included online ad networks, metrics companies, and social networks such as Scorecard Research ("Scorecard") (an online market research company), Facebook (the online social network), DoubleClick (an online ad network), Google Analytics (an online web analytics company), and QuantCast (an online ad network and web analytics company).

The information transmitted to Scorecard and Facebook included information that identified Plaintiffs and Class Members personally. As to Facebook, Hulu included their Facebook IDs, connecting the video content information to Facebook's personally identifiable user registration information. As to Scorecard, Hulu provided Plaintiffs' "Hulu profile identifiers" linked to their "individual Hulu profile pages that included name, location, preference information designated by the user as private, and Hulu username (which, in the case of many individuals, is the same screen name used in other online environments.)" . . . .

Plaintiffs allege that Hulu "knowingly and without . . . [their] consent disclosed to third parties . . . [their] video viewing selections and personally identifiable information, knowing that such disclosure included the disclosure of [their] personally identifying information . . . and their requests for and/or obtaining of specific video materials and/or services from Hulu," in violation of the Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710(b)(1).

The Act prohibits a "video tape service provider" from (1) knowingly disclosing to any person (2) personally identifiable information concerning any consumer of such provider (3) except for certain disclosures—such as to the consumer or law enforcement—allowed under section 2710(b)(2). 18 U.S.C. § 2710. "'Personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services." Such disclosures are not prohibited if they are "incident to the ordinary course of business" of the video tape service provider. The VPPA defines "ordinary course of business" as "debt collection activities, order fulfillment, request processing, and the transfer of ownership."

The VPPA defines "video tape service provider" as "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 visual materials."18 U.S.C. § 2710(a)(4).

Hulu does not deal in prerecorded video cassette tapes. Thus, whether Hulu is a "video tape service providers" turns on the scope of the phrase "similar audio visual materials."

Citing dictionary definitions, Hulu contends that "materials" are things "composed of physical matter." . . . As drafted, Hulu contends, the VPPA "only regulates businesses that sell or rent physical objects (i.e., 'video cassettes or other similar audio visual materials') . . . and not businesses that transmit digital content over the Internet." . . . Had Congress wanted to regulate businesses dealing in digital content, it would have defined "video tape service provider" to include businesses that "traffic in audio-visual information or data."

To this reader, a plain reading of a statute that covers videotapes and "similar audio visual materials" is about the video content, not about how that content was delivered (e.g. via the Internet or a bricks-and-mortar store). Still, the online streaming mechanism of delivery here did not exist when Congress enacted the statute in 1988. A dictionary definition helps some. The undersigned looked at the third edition of Oxford English Dictionary, which defines "material" both as "relating to substance" and as "Text or images in printed or electronic form; also with distinguishing word, as reading material, etc." . . .

Also, the Senate Report confirms that Congress was concerned with protecting the confidentiality of private information about viewing preferences regardless of the business model or media format involved. . . .

The court concludes that Congress used "similar audio video materials" to ensure that VPAA's protections would retain their force even as technologies evolve. . . .

The court denies Hulu's motion to dismiss.

IN RE HULU PRIVACY LITIGATION

2014 WL 1724344 (N.D. Cal. 2014)

BEELER, MAGISTRATE J. . . . In this putative class action, viewers of Hulu's on-line video content allege that Hulu wrongfully disclosed their video viewing selections and personal identification information to third parties such as metrics companies (meaning, companies that track data) and social networks, in violation of the Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710. . . .

The Act prohibits a "video tape service provider" from knowingly disclosing "personally identifiable information of a consumer of the provider" to third parties except under identified exceptions that do not apply here. See 18 U.S.C. § 2710. "The term 'personally identifiable information' includes information that identifies a person as having requested or obtained specific video materials or services from a video tape service provider." Id. § 2710(a)(3).

Hulu argues that it did not violate the VPPA because (I) it disclosed only anonymous user IDs and never linked the user IDs to identifying data such as a person's name or address; (II) it did not disclose the information "knowingly" and thus is not liable. . . .

The issue is whether Hulu's disclosures here (unique numeric identifications tied to video watching) are PII under the VPPA. The statute's plain language prohibits disclosure of information that "identifies a person" as having (in the Hulu context) viewed specific video content. 28 U.S.C. § 2710(a)(3). It does not say "identify by name" and thus plainly encompasses other means of identifying a person. Indeed, PII is not given one definition: "the term . . . includes information which identifies a person.". . .

The plain language of the statute suggests, and the Senate Report confirms, that the statute protects personally identifiable information that identifies a specific person and ties that person to particular videos that the person watched.

The issue then is whether the disclosures here are merely an anonymized ID or whether they are closer to linking identified persons to the videos they watched.

[Hulu made three types of disclosures: (1) video names and Hulu user ID numbers to comScore; (2) a unique ID number for each user created specifically for comScore's use; and (3) user IP addresses and cookies with a user's Facebook ID to Facebook, along with URL web addresses with video names in them.] . . .

Hulu . . . argues that the disclosure has to be the person's actual name. That position paints too bright a line. One could not skirt liability under the VPPA, for example, by disclosing a unique identifier and a correlated look-up table. The statute does not require a name. It defines PII as a term that "includes information which identifies a person." The legislative history shows Congress used the word "includes" when it defined PII to establish a minimum, but not exclusive, definition. It is information that "identifies a particular person as having engaged in a specific transaction with a video tape service provider" by retaining or obtaining specific video materials or services. It does not require identification by a name necessarily. One can be identified in many ways: by a picture, by pointing, by an employee number, by the station or office or cubicle where one works, by telling someone what "that person" rented. In sum, the statute, the legislative history, and the case law do not require a name, instead require the identification of a specific person tied to a specific transaction, and support the conclusion that a unique anonymized ID alone is not PII but context could render it not anonymous and the equivalent of the identification of a specific person. . . .

Hulu's liability here is based on the hypothetical that comScore could use the Hulu ID to access the Hulu user's profile page to obtain the user's name. Hulu characterizes this argument as "reverse engineering" its data. The idea is that comScore could capture the data from the watch page, extract the relevant information (the video name and Hulu User ID), and plug the data into the standard-format URL for the profile page to capture the user's name from that page. There is no evidence that comScore did this. The issue is only that it could. . . .

. . . [The evidence] does not suggest any linking of a specific, identified person and his video habits. The court grants summary judgment in Hulu's favor on this theory. . . .

[Regarding the Facebook disclosures,] Hulu argues that it never sent the "actual" name of any Facebook user. Instead, the name came from the user's web browser and the interaction that Facebook had with its users. . . .

It may be true—as Hulu says—that accessing a remote browser involves sending that browser's cookies. But according to Plaintiffs' expert, it was straightforward to develop a webpage that would not communicate information to Facebook. Put another way, it was not necessary to send the "Facebook user" cookies, and they were sent because Hulu chose to include the Like button on watch pages. . . .

Hulu argues that it needed to send an actual name to be liable and that it sent only cookies. The statute does not require an actual name and requires only something akin to it. If the cookies contained a Facebook ID, they could show the Hulu user's identity on Facebook. . . .

Hulu also argues that there is no evidence that Facebook took any actions with the cookies after receiving them. It also says that there is no evidence that Facebook tied its Facebook user cookies to the URL for the watch page (and the accompanying title). In contrast to comScore, where the user was not tied to the video in one transmission, the transmission to Facebook included the video name and Facebook user cookies. Thus, the link between user and video was more obvious. But Hulu's point is that the information really was not disclosed to Facebook in the sense that the information about Judge Bork's video viewing was disclosed to the Washington Post.

Whether this link was the equivalent of a disclosure under the VPPA depends on the facts. One can think of analogies in a paper world. Throwing Judge Bork's video watch list in the recycle bin is not a disclosure. Throwing it in the bin knowing that the Washington Post searches your bin every evening for intelligence about local luminaries might be. The issue is whether Hulu made a "knowing" disclosure.

The statute requires a "knowing" disclosure "to any person." See 18 U.S.C. § 2710(b)(1). The emphasis is on disclosure, not comprehension by the receiving person. Thus, the Seventh Circuit held that the practice of placing PII on parking tickets in the view of the public was a disclosure that violated the analogous Driver's Privacy Protection Act, regardless of whether anyone viewed the PII. *See Senne v. Village of Palatine Ill.*, 695 F.3d 597 (7th Cir.2012) (en banc). By analogy, if a video store knowingly hands a list of Judge Bork's rented videos to a Washington Post reporter, it arguably violates the VPPA even if the reporter does not look at the list. . . .

. . . [A]rguing that transmitting cookies is just the normal way that webpages and the Like button load is not enough to negate knowledge or show the absence of evidence about knowledge. . . .

The court denies Hulu's summary judgment motion regarding the disclosures to Facebook. . . .

NOTES & QUESTIONS

1. ***What Is a "Video Tape Service Provider"?*** The court holds that Hulu is a videotape service provider, even though the statutory language refers to videotapes and was written in 1994, long before online streaming video. Should the phrase "rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials" be interpreted broadly as the court interprets it?
2. ***What Is PII?*** The second opinion excerpted above involves what constitutes personally identifiable information (PII) under the VPPA. The court recognizes that the VPPA does not require actual names in order for a disclosure to be of PII — disclosing an ID could be the "equivalent to the identification of a specific person" depending upon the context. However, the court grants summary judgment to Hulu regarding the comScore disclosure because of a lack of evidence comScore was re-identifying the data by linking the ID to a

person's name. Why is sending the cookies to Facebook different? The court writes:

> Hulu also argues that there is no evidence that Facebook took any actions with the cookies after receiving them. It also says that there is no evidence that Facebook tied its Facebook user cookies to the URL for the watch page (and the accompanying title). In contrast to comScore, where the user was not tied to the video in one transmission, the transmission to Facebook included the video name and Facebook user cookies. Thus, the link between user and video was more obvious.

Do you agree with this distinction? In dismissing comScore, the court also focused on the lack of actions comScore took after receiving the ID information. The court noted that "if a video store knowingly hands a list of Judge Bork's rented videos to a Washington Post reporter, it arguably violates the VPPA even if the reporter does not look at the list." Suppose a video store hands a list of rented videos to a *Washington Post* reporter with a unique ID number of the customer on the list. The *Washington Post* reporter can readily look up the unique ID number to figure out who the individual is. Why is the reporter who does not look at the list treated differently from the reporter who does not look up the unique ID number?

(b) The Cable Communications Policy Act

In 1984, Congress passed the Cable Communications Policy Act (CCPA or "Cable Act"), Pub. L. No. 98-549. The Act applies to cable operators and service providers. 47 U.S.C. § 551(a)(1).

Notice and Access. The Cable Act requires cable service providers to notify subscribers (in a written privacy policy) of the nature and uses of personal information collected. § 551(a)(1). Subscribers must have access to their personal data held by cable operators. § 551(d).

Limitations on Data Collection. Cable operators "shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned." § 551(b)(1).

Limitations on Data Disclosure. Cable operators cannot disclose personally identifiable information about any subscriber without the subscriber's consent:

> [A] cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator. § 551(c)(1).

However, cable operators can disclose personal data under certain circumstances, such as when necessary for a "legitimate business activity" or pursuant to a court order if the subscriber is notified. Cable operators may disclose

subscriber names and addresses if "the cable operator has provided the subscriber the opportunity to prohibit or limit such disclosure." § 551(c)(2).

Data Destruction. Cable operators must destroy personal data if the information is no longer necessary for the purpose for which it was collected. § 551(e).

Government Access to Cable Information. Pursuant to § 551(h):

> A governmental entity may obtain personally identifiable information concerning a cable subscriber pursuant to a court order only if, in the court proceeding relevant to such court order —
>
> (1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and
>
> (2) the subject of the information is afforded the opportunity to appear and contest such entity's claim.

Note that a court order to obtain cable records requires "clear and convincing evidence," a standard higher than probable cause. There is no exclusionary rule for information obtained in violation of the Cable Act.

Enforcement. The Cable Act provides for a private cause of action and actual damages, with a minimum of $1,000 or $100 for each day of the violation, whichever is higher. The plaintiff can collect any actual damages that are more than the statutory minimum. Further, the Cable Act provides for punitive damages and attorneys' fees. § 551(f).

Cable Internet Service. Section 211 of the USA PATRIOT Act amended the Cable Act, 47 U.S.C. § 551(c)(2)(D), to provide disclosure to a government entity under federal wiretap law when the government seeks information from cable companies except that "such disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator." This provision of the PATRIOT Act will not sunset.

New Cable Services and Products? In March 2011, the *Wall Street Journal* reported on the testing by cable companies of new systems that are designed to show households highly targeted ads.[72] The goal is to "emulate the sophisticated tracking widely used on people's personal computers with new technology that reaches the living room." In one test of Cablevision's technology, for example, the U.S. Army used it to target four different recruitment ads to different categories of viewers. In many of these systems, companies generally seek to remove personal data, including names, before data is sent to third party companies who match ads to households.

In August 2014, the *Washington Post* predicted that the cable industry was about to start serving targeted ads on a large scale. It discussed how a cable-owned service, called NBCU+, was planning to combine cable subscriber information

[72] Jessica E. Vascellaro, *TV's Next Wave: Tuning into You*, Wall St. J., Mar. 7, 2011.

with data from other sources, "such as loyalty card purchases, box office sales, and even car registrations."[73] The plan was said likely to involve purchasing data from data brokers, such as Acxiom and Experian.

Does these practices comport with the Cable Act?

2. INTERNET USE AND ELECTRONIC COMMUNICATIONS

(a) The Children's Online Privacy Protection Act

Passed in 1998, the Children's Online Privacy Protection Act (COPPA), Pub. L. No. 106-170, 15 U.S.C. §§ 6501–6506, regulates the collection and use of children's information by Internet websites. In January 2013, the FTC issued an important amendment to its COPPA Rule, which it included in a complete re-issued Final COPPA Rule. 16 C.F.R. Part 312. These Rules took effect in July 2013.

Scope. COPPA applies to "an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child." 15 U.S.C. § 6502(a)(1). COPPA only applies to websites that collect personal information from children under age 13. § 6502(1). COPPA does not apply to information collected from adults about children under 13; it only applies to personal data collected *from* children themselves.

Personal Information. In 2013, the FTC clarified that "personal information" under COPPA includes a voice, audio, image file containing a child's voice and/or image; geolocation data that reveals a street name plus city, or equally revealing information; online contact information such as a screen name or user name, persistent identifiers that recognize users across time and sites or services, such as an IP address or device serial number. COPPA Final Rule, 78 Fed. Reg. 3971 (Jan. 17, 2013), 16 C.F.R. § 312.

Collection of Personal Information. The "collection" of personal information is defined broadly. It means "the gathering of any personal information from a child by any means, including but not limited to: (1) Requesting, prompting, or encouraging a child to submit personal information online; (2) Enabling a child to make personal information publicly available in identifiable form." 16 C.F.R. § 312.2.

Notice. Children's websites must post privacy policies, describing "what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information." § 6502(b)(1)(A)(i).

[73] Brian Fung, *Blogs: The Switch, Targeted Ads Are About to Take Over Your TV*, Wash. Post (Jan. 31, 2014).

Consent. Children's websites must "obtain verifiable parental consent for the collection, use or disclosure of personal information from children." § 6502(b)(1)(A)(ii). Websites cannot condition child's participation in a game or receipt of a prize on the disclosure of more personal information than is necessary to participate in that activity. § 6502(b)(1)(C). When information is not maintained in retrievable form, then consent is not required. § 6502(b)(2).

Right to Restrict Uses of Personal Information. If parent requests it, the operator must provide to the parent a description of the "specific types of personal information collected," the right to "refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child," and the right to "obtain any personal information collected from the child." § 6502(b)(1)(B).

Liability When Sites Operate in Connection with Third Parties. As of the 2013 rule change, both hosts of sites and third parties operating through sites are subject to enforcement under COPPA. Hosts regulated by COPPA are strictly liable for the activities of third parties operating on their site if the third party is an agent of the regulated service or the primary regulated service receives a benefit from a third party. The third party is liable if it has "actual knowledge" that the host site is directed to children. For example, a website using ads from an ad network is strictly liable for information collected by the ad network. The ad network would be liable if it has actual knowledge that the website is directed to children. *See* COPPA Final Rule, 16 § C.F.R. 312.

Enforcement. Violations of COPPA are "treated as a violation of a rule defining an unfair or deceptive act or practice" under 15 U.S.C. § 57a(a)(1)(B). Thus, the FTC enforces the law and can impose fines up to $16,000 per violation. The amount of the fine depends upon a number of factors including "the egregiousness of the violations, whether the operator has previously violated the Rule, the number of children involved, the amount and type of personal information collected, how the information was used, whether it was shared with third parties, and the size of the company."[74]

There is no private cause of action for violations of COPPA. States can bring civil actions for violations of COPPA in the interests of its citizens to obtain injunctions and damages. § 6504.

Preemption. COPPA preempts state law. § 6502(d).

Safe Harbor. If an operator follows self-regulatory guidelines issued by marketing or online industry groups that are approved by the FTC, then the COPPA requirements will be deemed satisfied. § 6503.

Should COPPA be extended to apply to everyone, not just children? Should there be a private cause of action under COPPA? Note that COPPA only applies

[74] FTC, *Complying with COPPA: Frequently Asked Questions* (July 16, 2014), http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions.

when a website has "actual knowledge" that a user is under 13 or operates a website specifically targeted to children. Is this too limiting? Would a rule dispensing with the "actual knowledge" requirement be feasible?[75]

UNITED STATES V. PATH, INC.

2012 WL 7006381 (N.D. Cal. 2012)

COMPLAINT

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("FTC" or "Commission"), for its Complaint alleges:

1. Plaintiff brings this action under . . . the Children's Online Privacy Protection Act of 1998 ("COPPA") . . .

7. Defendant Path, Inc. ("Path") . . . develops, markets, distributes, or sells software applications for mobile devices to consumers throughout the U.S. and provides online services to users of its applications. From at least 2010, Defendant has operated a social networking online service that is accessible worldwide on the Internet through a website and mobile applications. . . .

10. Defendant describes its social networking service as "the smart journal that helps you share life with the ones you love," and allows users to keep a journal about "moments" in the user's life and to share that journal with a network of up to 150 persons. Through the Path App, the user can upload, store and share photos, written "thoughts," the user's location, and the names of songs to which the user is listening. On the "About" page of its website, Defendant describes its "Values" and espouses that "Path should be private by default. Forever. You should always be in control of your information and experience."

11. At all times relevant to this Complaint, when a user registers for Defendant's social networking service, the user must provide an email address, a first name, and a last name. The user's email address serves as his or her login identity. At registration, the user is also invited to provide gender, phone number, and date of birth. The Path App for iOS has been downloaded and installed over 2.5 million times. . . .

20. In addition to its Path App for iOS, Defendant's social networking service is also accessible through a Path App for Google, Inc.'s Android operating system, and, until December 2011, through Defendant's website, path.com. The Path App for iOS, the Path App for Android, and the Defendant's website were all intended for a general audience, but also attracted a significant number of children.

21. As discussed in Paragraph 11, when a user registered for the Defendant's social networking service, whether through one of the Path Apps or through Defendant's website, the user was required to provide an email address, a first name, and a last name, and was invited to provide gender, phone number, and date of birth.

---

[75] For more information about COPPA, see Dorothy A. Hertzel, Note, *Don't Talk to Strangers: An Analysis of Government and Industry Efforts to Protect Child's Privacy Online*, 52 Fed. Comm. L.J. 429 (2000).

22. From November 14, 2010, through May 4, 2012, Defendant accepted registrations from users who entered a date of birth indicating that the user was under the age of 13. As a result, Defendant knowingly collected email address, first name, last name, date of birth, and if provided, gender and phone number, from approximately 3,000 children under age 13. Defendant, therefore, was an "operator" as defined in the Rule.

23. From November 29, 2011, through February 8, 2012, Defendant also knowingly collected from these children the following personal information for each contact in the child's mobile device address book, if available: first name, last name, address, phone numbers, email addresses, and date of birth.

24. A child who registered through the Path App or Defendant's website was able to create a journal and upload, store and share photos, written "thoughts," the child's precise location, and the names of songs to which the child was listening. In fact, each time a child uploaded a photo or posted a "thought," the Path App would invite the child to also share his or her location through the application's geo-location tracking feature and the names of any friends that were with the child when the photo was taken or the thought was posted. Likewise, if the child decided to share his or her location through the application's geo-location tracking feature, the Path App would invite the child to also share the names of friends that were with the child at that location, and prompt the child to add a "thought." The child could also comment on the posts of other users in the child's network.

25. Until May 4, 2012, Defendant knowingly collected children's personal information and enabled children to publicly disclose their personal information through the Defendant's social networking service.

26. Defendant's online notice of its information practices did not clearly, completely, or accurately disclose all of Defendant's information collection, use, and disclosure practices for children, as required by the Rule.

27. Defendant did not provide parents with a direct notice of its information practices prior to collecting, using, or disclosing children's personal information.

28. Defendant did not obtain verifiable consent from parents prior to collecting, using, or disclosing children's personal information.

29. In approximately 3,000 instances, Defendant knowingly collected, used, and/or disclosed personal information from children in violation of the Children's Online Privacy Protection Rule. . . .

34. In numerous instances, in connection with operating its Path App for iOS, its Path App for the Android operating system, and its website, path.com, Defendant collected, used, and/or disclosed, with actual knowledge, personal information online from children younger than age 13. Defendant failed to: (1) provide sufficient notice on its website or online services of the information it collects online from children, how it uses such information, and its disclosure practices, among other required content; (2) provide direct notice to parents of the information Defendant collects online from children, how it uses such information, and its disclosure practices for such information, among other required content; and (3) obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children. . . .

NOTES & QUESTIONS

1. ***Settlement.*** Path settled with the FTC, agreeing to destroy the data it had collected about children. Path also agreed to pay a civil payment of $800,000.
2. ***Inadvertently Triggering COPPA.*** Path's online service was not directed at children under 13; rather, it was for all users. It triggered COPPA because it collected birth dates, thus giving it actual knowledge that some users were under 13. Is it fair to punish Path for what might have been an inadvertent triggering of COPPA?
3. ***Restricting Use to Users 13 Years or Older.*** Some websites seek to avoid triggering COPPA by requiring users to be 13 or older. For example, Facebook states:

> Facebook requires everyone to be at least 13 years old before they can create an account (in some jurisdictions, this age limit may be higher). Creating an account with false info is a violation of our terms. This includes accounts registered on the behalf of someone under 13

The result of COPPA thus means fewer sites that allow users under 13. Is this result desirable?

The reality is, however, that many children under 13 lie about their age in order to sign up for Facebook accounts. In June 2011, Consumer Reports found that "more than one-third of the 20 million minors who actively used Facebook in the past year" were under 13.[76] This meant 7.5 million users of Facebook who were younger than 13. It stated: "Parents of kids 10 and younger on Facebook seem to be largely unconcerned." The magazine also warned, "Ten-year-olds need protection from . . . hazards that might lurk on the Internet, such as links that might infect their computer with malware and invitations from strangers, not to mention bullies."

To what extent should Facebook have an obligation to make it harder for children under 13 to sign up deceitfully? For all the children who do lie about their age, is Facebook just putting its head in the sand?

One possible solution is to remove the "actual knowledge" prong of COPPA and only apply the law to websites specifically directed at children. But would that be too limiting of COPPA and allow too much of an end-run around its protections?

4. ***FTC Enforcement Actions.*** The FTC has engaged in several 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. In 2011, the FTC received its largest civil settlement yet under COPPA. Playdom, an operator of online virtual worlds, agreed to pay $3 million to settle FTC charges that it had violated COPPA. The company was alleged to have illegally collected and disclosed personal information from hundreds of thousands of children under age 13 without their parents' prior consent.

[76] *That Facebook Friend Might Be 10 Years Old, and Other Troubling News*, Consumer Reports (June 2011).

In its complaint, the FTC stated that Playdom violated its stated privacy policy by collecting children's personal information and enabling children to publicly disclose this information through their personal profile pages and in community forums at its websites. The company also did not take necessary steps "to provide parents with a direct notice of [its] information practices prior to collecting, using, or disclosing children's personal information" and to collect "verifiable consent from parents." The FTC tallied no fewer than 1.2 million instances of the company's collection, use, and/or disclosure of personal information in violation of COPPA.

As a further example, the FTC announced a settlement in 2006 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 2011, in *United States v. W3 Innovations, LLC,* No. CV-11-03958-PSG (Aug. 12, 2011), the FTC settled an action against a developer of children's gaming apps for the iPhone and iPod. W3 Innovations (doing business as Broken Thumbs Apps) failed to have a privacy policy or to obtain parental consent before collecting and disclosing children's personal data. Under the settlement, W3 was fined $50,000 and ordered to delete all information collected in violation of COPPA.

5. ***Is COPPA Too Paternalistic?*** Consider the following critique of COPPA by Anita Allen:

> Not all parents welcome the veto power COPPA confers. New power has meant new responsibility. The statute forces parents who would otherwise be content to give their children free rein over their computers to get involved in children's use of Internet sites that are geared toward children and collect personal information. . . .
>
> Prohibiting voluntary disclosures by children lacking parental consent in situations in which they and their parents may be indifferent to privacy losses and resentful of government intervention, COPPA is among the most paternalistic and authoritarian of the federal privacy statutes thus far.[77]

More recently, Allen has wondered whether young adults might also need paternalistic laws.[78] At the same time, she concedes, "Sharing data is the way of the contemporary world. There is no chance the United States government will intervene in a strict censorship mode to curb radical forms of self-disclosure online." On a pessimistic note, Allen also notes:

[77] Anita L. Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 Hous. L. Rev. 751, 752-53, 768-69, 775-76 (2001).

[78] Anita L. Allen, *Unpopular Privacy* 190-94 (2011).

> [COPPA] could be viewed as part of a nation's formative educational project: the young are to be taught the value of privacy by imposing privacy protection rules limiting their choices until they are old enough to choose responsibly. But it will be difficult for children to get the message that privacy is a duty of self-care if they closely observe the actual behavior of teens and young adults. Everyone under the age of forty seems to be freely sharing personal facts, ideas, fantasies, and revealing images of themselves all the time.

Is COPPA doomed by a decline of modesty about self-revelation on the Internet? What role, if any, should the law play in nudging or coercing people to protect their own privacy?

(b) The Electronic Communications Privacy Act

In several cases, plaintiffs have attempted to use the Electronic Communications Privacy Act (ECPA) to prevent certain kinds of information collection, use, and disclosure by commercial entities. Recall from Chapter 3 that EPCA consists of three acts: (1) the Wiretap Act, 18 U.S.C. §§ 2510–2522, which regulates the interception of communications; (2) the Stored Communications Act (SCA), 18 U.S.C. §§ 2701–2711, which regulates communications in storage and ISP subscriber records; and (3) the Pen Register Act, 18 U.S.C. §§ 3121–3127, which regulates the use of pen register and trap and trace devices. The attempts to use ECPA to regulate commercial entities using personal information primarily seek to use the Wiretap Act or the SCA.

IN RE GOOGLE, INC. GMAIL LITIGATION

2013 WL 5423918 (N.D. Cal. 2013)

KOH, J. In this consolidated multi-district litigation, Plaintiffs . . . allege that Defendant Google, Inc., has violated state and federal antiwiretapping laws in its operation of Gmail, an email service. Before the Court is Google's Motion to Dismiss Plaintiffs' Consolidated Complaint. . . .

Plaintiffs challenge Google's operation of Gmail under state and federal anti-wiretapping laws. The Consolidated Complaint seeks damages on behalf of a number of classes of Gmail users and non–Gmail users for Google's interception of emails over a period of several years. . . . Plaintiffs allege . . . that in all iterations of Google's email routing processes since 2008, Google has intercepted, read and acquired the content of emails that were sent or received by Gmail user while the emails were in transit. . . .

Plaintiffs further allege that Google used these . . . data to create user profiles and models. Google then allegedly used the emails, affiliated data, and user profiles to serve their profit interests that were unrelated to providing email services to particular users. . . .

Gmail implicates several different, but related, systems of email delivery, three of which are at issue here. The first is a free service, which allows any user to register for an account with Google to use Gmail. This system is supported by advertisements, though users can opt-out of such advertising or access Gmail accounts in ways that do not generate advertising, such as accessing email on a smartphone.

The second is Google's operation of email on behalf of Internet Service Providers ("ISPs"). Google, through its Google Apps Partner program, enters into contracts with ISPs, such as Cable One, to provide an email service branded by the ISP. The ISP's customers can register for email addresses from their ISP (such as "@mycableone.com"), but their email is nevertheless powered by Google through Gmail.

Third, Google operates Google Apps for Education, through which Google provides email on behalf of educational organizations for students, faculty, staff, and alumni. These users receive "@name.institution.edu" email addresses, but their accounts are also powered by Google using Gmail. *Id.* Universities that are part of Google Apps for Education require their students to use the Gmail–provided service.

Google Apps users, whether through the educational program or the partner program, do not receive content-based ads but can opt in to receiving such advertising. Google processes emails sent and received from all Gmail users, including Google Apps users, in the same way except that emails of users who do not receive advertisements are not processed through Google's advertising infrastructure, which attaches targeted advertisements to emails. . . . [E]mails to and from users who did not receive advertisements are nevertheless intercepted to create user profiles. . . .

The operation of the Gmail service implicates several legal agreements. Gmail users were required to agree to one of two sets of Terms of Service during the class periods. The first Terms of Service was in effect from April 16, 2007, to March 1, 2012, and the second has been in effect since March 1, 2012. The 2007 Terms of Service stated that:

> Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service. For some Services, Google may provide tools to filter out explicit sexual content. These tools include the SafeSearch preference settings.... In addition, there are commercially available services and software to limit access to material that you may find objectionable.

A subsequent section of the 2007 Terms of Service provided that "[s]ome of the Services are supported by advertising revenue and may display advertisements and promotions" and that "[t]hese advertisements may be content-based to the content information stored on the Services, queries made through the Service or other information."

The 2012 Terms of Service deleted the above language and stated that users "give Google (and those [Google] work[s] with) a worldwide license to use . . . , create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), . . . and distribute such content."

Both Terms of Service reference Google's Privacy Policies, which have been amended three times thus far during the putative class periods. These Policies, which were largely similar, stated that Google could collect information that users

provided to Google, cookies, log information, user communications to Google, information that users provide to affiliated sites, and the links that a user follows. The Policies listed Google's provision of "services to users, including the display of customized content and advertising" as one of the reasons for the collection of this information.

Google also had in place Legal Notices, which stated . . . that Google "will not use any of [users'] content for any purpose except to provide [users] with the service." . . .

Importantly, Plaintiffs who are not Gmail or Google Apps users are not subject to any of Google's express agreements. Because non-Gmail users exchange emails with Gmail users, however, their communications are nevertheless subject to the alleged interceptions at issue in this case.

Plaintiffs bring these cases alleging that Google, in the operation of its Gmail system, violated federal and state anti-wiretapping laws. . . .

The Wiretap Act, as amended by the ECPA, generally prohibits the interception of "wire, oral, or electronic communications." 18 U.S.C. § 2511(1); More specifically, the Wiretap Act provides a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a); *see id.* § 2520 (providing a private right of action for violations of § 2511). The Act further defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."

Plaintiffs contend that Google violated the Wiretap Act in its operation of the Gmail system by intentionally intercepting the content of emails that were in transit to create profiles of Gmail users and to provide targeted advertising. . . .

1. *"Ordinary Course of Business" Exception.* Google first contends that it did not engage in an interception because its reading of users' emails occurred in the ordinary course of its business. . . . The Court finds that the ordinary course of business exception is narrow. The exception offers protection from liability only where an electronic communication service provider's interception facilitates the transmission of the communication at issue or is incidental to the transmission of such communication. Specifically, the exception would apply here only if the alleged interceptions were an instrumental part of the transmission of email. Plaintiffs have alleged, however, that Google's interception is not an instrumental component of Google's operation of a functioning email system. In fact, Google's alleged interception of email content is primarily used to create user profiles and to provide targeted advertising—neither of which is related to the transmission of emails. The Court further finds that Plaintiffs' allegations that Google violated Google's own agreements and internal policies with regard to privacy also preclude application of the ordinary course of business exception. . . .

The narrow construction of "ordinary course of business" is most evident in section 2510(5)(a)(i) cases where an employer has listened in on employees' phone calls in the workplace. These cases suggest that an employer's eavesdropping on an employee's phone call is only permissible where the employer has given notice to the employee. Further, these cases have suggested that an employer may only listen to an employee's phone call for the narrow purpose of determining whether a call is for personal or business purposes. . . .

In light of the statutory text, case law, statutory scheme, and legislative history concerning the ordinary course of business exception, the Court finds that the section 2510(5)(a)(ii) exception is narrow and designed only to protect electronic communication service providers against a finding of liability under the Wiretap Act where the interception facilitated or was incidental to provision of the electronic communication service at issue. Plaintiffs have plausibly alleged that Google's reading of their emails was not within this narrow ordinary course of its business. Specifically, Plaintiffs allege that Google intercepts emails for the purposes of creating user profiles and delivering targeted advertising, which are not instrumental to Google's ability to transmit emails. . . . Plaintiffs support their assertion by suggesting that Google's interceptions of emails for targeting advertising and creating user profiles occurred independently from the rest of the email-delivery system. . . .

Accordingly, the Court denies Google's Motion to Dismiss based on the section 2510(5)(a)(ii) exception.

2. *Consent.* Google's second contention with respect to Plaintiffs' Wiretap Act claim is that all Plaintiffs consented to any interception of emails in question in the instant case. Specifically, Google contends that by agreeing to its Terms of Service and Privacy Policies, all Gmail users have consented to Google reading their emails Google further suggests that even though non–Gmail users have not agreed to Google's Terms of Service or Privacy Policies, all non–Gmail users impliedly consent to Google's interception when non-Gmail users send an email to or receive an email from a Gmail user.

If either party to a communication consents to its interception, then there is no violation of the Wiretap Act. 18 U.S.C. § 2511(2)(d). Consent to an interception can be explicit or implied, but any consent must be actual. Courts have cautioned that implied consent applies only in a narrow set of cases. The critical question with respect to implied consent is whether the parties whose communications were intercepted had adequate notice of the interception. That the person communicating knows that the interceptor has the *capacity* to monitor the communication is insufficient to establish implied consent. Moreover, consent is not an all-or-nothing proposition. Rather, "[a] party may consent to the interception of only part of a communication or to the interception of only a subset of its communications." . . .

In its Motion to Dismiss, Google marshals both explicit and implied theories of consent. Google contends that by agreeing to Google's Terms of Service and Privacy Policies, Plaintiffs who are Gmail users expressly consented to the interception of their emails. Google further contends that because of the way that email operates, even non-Gmail users knew that their emails would be intercepted, and accordingly that non-Gmail users impliedly consented to the interception. Therefore, Google argues that in all communications, both parties—regardless of whether they are Gmail users—have consented to the reading of emails. The Court rejects Google's contentions with respect to both explicit and implied consent. Rather, the Court finds that it cannot conclude that any party—Gmail users or non-Gmail users—has consented to Google's reading of email for the purposes of creating user profiles or providing targeted advertising.

Google points to its Terms of Service and Privacy Policies, to which all Gmail and Google Apps users agreed, to contend that these users explicitly consented to

the interceptions at issue. The Court finds, however, that those policies did not explicitly notify Plaintiffs that Google would intercept users' emails for the purposes of creating user profiles or providing targeted advertising.

Section 8 of the Terms of Service that were in effect from April 16, 2007, to March 1, 2012, stated that "Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service." This sentence was followed by a description of steps users could take to avoid sexual and objectionable material. Later, section 17 of the Terms of Service stated that "advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information."

The Court finds that Gmail users' acceptance of these statements does not establish explicit consent. Section 8 of the Terms of Service suggests that content may be intercepted under a different set of circumstances for a different purpose—to exclude objectionable content, such as sexual material. This does not suggest to the user that Google would intercept emails for the purposes of creating user profiles or providing targeted advertising. Therefore, to the extent that section 8 of the Terms of Service establishes consent, it does so only for the purpose of interceptions to eliminate objectionable content. The Consolidated Complaint suggests, however, that Gmail's interceptions for the purposes of targeted advertising and creation of user profiles was separate from screening for any objectionable content. Because the two processes were allegedly separate, consent to one does not equate to consent to the other.

Section 17 of the Terms of Service—which states that Google's "advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information"—is defective in demonstrating consent for a different reason: it demonstrates only that Google has the *capacity* to intercept communications, not that it will. Moreover, the language suggests only that Google's advertisements were based on information "stored on the Services" or "queries made through the Services"—not information in transit via email. Plaintiffs here allege that Google violates the Wiretap Act, which explicitly protects communications in transit, as distinguished from communications that are stored. Furthermore, providing targeted advertising is only one of the alleged reasons for the interceptions at issue in this case. Plaintiffs also allege that Google intercepted emails for the purposes of creating user profiles. Section 17, to the extent that it suggests interceptions, only does so for the purposes of providing advertising, not creating user profiles. Accordingly, the Court finds that neither section of the Terms of Service establishes consent.

The Privacy Policies explicitly state that Google collects "user communications . . . *to Google*." This could mislead users into believing that user communications to each other or to nonusers were not intercepted and used to target advertising or create user profiles. As such, these Privacy Policies do not demonstrate explicit consent, and in fact suggest the opposite.

After March 1, 2012, Google modified its Terms of Service and Privacy Policy. The new policies are no clearer than their predecessors in establishing consent. The relevant part of the new Terms of Service state that when users upload content to Google, they "give Google (and those [Google] work[s] with) a worldwide license to use . . . , create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), . . . and distribute such content."

The Terms of Service cite the new Privacy Policy, in which Google states to users that Google "may collect information about the services that you use and how you use them, like when you visit a website that uses our advertising services or you view and interact with our ads and content. This information include [device information, log information, location information, unique application numbers, local storage, cookies, and anonymous identifiers]. The Privacy Policy further states that Google "use[s] the information [it] collect[s] from all [its] services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and [its] users. [Google] also use[s] this information to offer you tailored content—like giving you more relevant search results and ads." These new policies do not specifically mention the content of users' emails to each other or to or from non-users; these new policies are not broad enough to encompass such interceptions. Furthermore, the policies do not put users on notice that their emails are intercepted to create user profiles. The Court therefore finds that a reasonable Gmail user who read the Privacy Policies would not have necessarily understood that her emails were being intercepted to create user profiles or to provide targeted advertisements. Accordingly, the Court finds that it cannot conclude at this phase that the new policies demonstrate that Gmail user Plaintiffs consented to the interceptions.

Finally, Google contends that non-Gmail users—email users who do not have a Gmail account and who did not accept Gmail's Terms of Service or Privacy Policies—nevertheless impliedly consented to Google's interception of their emails to and from Gmail users, and to Google's use of such emails to create user profiles and to provide targeted advertising. Google's theory is that all email users understand and accept the fact that email is automatically processed. However, the cases Google cites for this far-reaching proposition hold only that the sender of an email consents to the intended recipients' recording of the email—not, as has been alleged here, interception by a third-party service provider. Google has cited no case that stands for the proposition that users who send emails impliedly consent to interceptions and use of their communications by third parties other than the intended recipient of the email. Nor has Google cited anything that suggests that by doing nothing more than receiving emails from a Gmail user, non–Gmail users have consented to the interception of those communications. Accepting Google's theory of implied consent—that by merely sending emails to or receiving emails from a Gmail user, a non–Gmail user has consented to Google's interception of such emails for any purposes—would eviscerate the rule against interception. The Court does not find that non-Gmail users who are not subject to Google's Privacy Policies or Terms of Service have impliedly consented to Google's interception of their emails to Gmail users.

Because Plaintiffs have adequately alleged that they have not explicitly or implicitly consented to Google's interceptions, the Court denies Google's Motion to Dismiss on the basis of consent. . . .

NOTES & QUESTIONS

1. ***Gmail's Business Model.*** Google offers Gmail for free to users and makes money from Gmail through targeted advertising. Google can fix its problems obtaining user consent by providing more explicit notice to Gmail account holders. But how should it deal with non-Gmail users who correspond with Gmail users? Does this problem make the business model unworkable? Is there a way to readily obtain the consent of non-Gmail users?
2. ***The Scope of the Wiretap Act.*** In *Joffe v. Google, Inc.*, 746 F.3d 920 (9th Cir. 2013), plaintiffs sued Google alleging that it violated the Wiretap Act by collecting data from unencrypted Wi-Fi networks. Google argued that data transmitted via Wi-Fi is a "radio communication" that is "readily accessible to the general public" and exempt from the Wiretap Act. The court rejected Google's argument.
3. ***Does ECPA Prohibit Cookies?*** When a person interacts with a website, the site can record certain information about the person, such as what parts of the website the user visited, what the user clicked on, and how long the user spent reading different parts of the website. This information is called "clickstream data."

   Websites use "cookies" to identify particular users.[79] A cookie is a small text file that is downloaded into the user's computer when a user accesses a Web page. The text in a cookie, which is often encoded, usually includes an identification number and several other data elements, such as the website and the expiration date. The cookie lets a website know that a particular user has returned. The website can then access any information it collected about that individual on her previous visits to the website. Cookies can also be used to track users as they visit multiple websites.

   In *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001), a group of plaintiffs challenged DoubleClick's use of cookies under the Stored Communications Act (SCA) and Wiretap Act. In 2001, DoubleClick was the leading company providing online advertising. DoubleClick helps advertisers distribute advertisements to websites based on information about specific web surfers. When a person visits a DoubleClick-affiliated website, DoubleClick places a cookie on that person's computer. As the person visits other sites that use DoubleClick, it builds a profile of that person's Web surfing activity. DoubleClick then can target ads to specific people based on their profile. For example, suppose a news website uses DoubleClick. A person visits the news website. The website checks with DoubleClick to see if DoubleClick recognizes the person. If the person's computer has a DoubleClick cookie, DoubleClick then looks up the profile associated with the cookie and sends the website advertisements tailored to that person's interests. Suppose Person A likes tennis and Person B likes golf. When Person A goes to the news website, a banner ad for tennis might appear. When Person B visits the same site, a banner ad for golf might appear.

[79] For a discussion of the *DoubleClick* case, see Tal Zarsky, *Cookie Viewers and the Undermining of Data-Mining: A Critical Review of the DoubleClick Settlement*, 2002 Stan. Tech. L. Rev. 1.

The plaintiffs in the *DoubleClick* case raised an SCA claim and a Wiretap Act claim. Regarding the SCA claim, the Act provides:

> [W]hoever (1) intentionally accesses without authorization a facility through which an electronic information service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . access to a wire or electronic communication while it is in electronic storage in such system shall be punished. . . . 18 U.S.C. § 2701(a).

Although the court ultimately concluded that the SCA did not apply, its reasoning was very controversial. The court first held that an individual's computer, when connected to the Internet, was a "facility through which an electronic information service is provided." This means that when DoubleClick accessed cookies on people's computers, it was "intentionally access[ing] without authorization a facility through which an electronic information service is provided." However, the consent exception to this provision of the SCA is that "users" may authorize access "with respect to a communication of or intended for that user." § 2701(c). The individuals whose computers were accessed were obviously users, and they did not consent. But the websites that the users visited that used DoubleClick cookies were also "users" in the court's interpretation, and they consented. Only one party needs to consent for the SCA consent exception to apply.

Moreover, the court noted that the SCA only applies to "temporary, intermediate storage of a wire or electronic communication," § 2510(17), and that DoubleClick's cookies were not "temporary" because they exist on people's hard drives for a virtually infinite time period.

Commentators argue that the court's application of the SCA is wrong because a "facility" refers to an Internet Service Provider, not an individual computer. Consider Orin Kerr:

> [T]he Stored Communications Act regulates the privacy of Internet account holders at ISPs and other servers; the law was enacted to create by statute a set of Fourth Amendment-like set of rights in stored records held by ISPs. The theory of the *Doubleclick* plaintiffs turned this framework on its head, as it attempted to apply a law designed to give account holders privacy rights in information held at third-party ISPs to home PCs interacting with websites.[80]

In *In re Pharmatrak Inc. Privacy Litigation*, 220 F. Supp. 2d 4 (D. Mass. 2002), aff'd 392 F.3d 9 (1st Cir. 2003), the court interpreted the SCA as Kerr suggests, holding that an individual's personal computer was not a "facility" under the SCA.

Regarding the Wiretap Act claim, DoubleClick conceded, for the purposes of summary judgment, that it had "intercepted" electronic communications. Orin Kerr also takes issue with this concession:

> [T]he Wiretap Act prohibits a third-party from intercepting in real-time the contents of communications between two parties unless one of the two parties consents. This law had no applicability to Doubleclick's cookies, as the cookies

[80] Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 Hastings L.J. 805, 831 (2003).

did not intercept any contents and did not intercept anything in real-time. The cookies merely registered data sent to it from Doubleclick's servers.[81]

DoubleClick argued that even if it intercepted electronic communications, the consent exception applied, since one party (the websites using DoubleClick) consented. The court agreed. The consent exception, however, does not apply if even with consent the "communication is intercepted for the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). The court concluded: "DoubleClick's purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money by providing a valued service to commercial Web sites."

4. ***Web Bugs.*** Beyond cookies, another device for collecting people's data is called a "Web bug." As one court describes it, Web bugs (or "action tags") are very tiny pixels on a website that can record how a person navigates around the Internet. Unlike a cookie, which can be accepted or declined by a user, a Web bug is a very small graphic file that is secretly downloaded to the user's computer. Web bugs enable the website to monitor a person's keystrokes and cursor movement. Web bugs can also be placed in e-mail messages that use HTML, or HyperText Markup Language. E-mail using HTML enables users to see graphics in an e-mail. A Web bug in an e-mail message can detect whether the e-mail was read and to whom it was forwarded. According to computer security expert Richard M. Smith, a Web bug can gather the IP address of the computer that fetched the Web bug; the URL of the page that the Web bug is located on; the URL of the Web bug image; the time the Web bug was viewed; the type of browser that fetched the Web bug image; and a previously set cookie value. Is the use of a Web bug a violation of federal electronic surveillance law?

DYER V. NORTHWEST AIRLINES CORP.

334 F. Supp. 2d 1196 (D.N.D. 2004)

HOVLAND, C.J. . . . Following September 11, 2001, the National Aeronautical and Space Administration ("NASA") requested system-wide passenger data from Northwest Airlines for a three-month period in order to conduct research for use in airline security studies. Northwest Airlines complied and, unbeknownst to its customers, provided NASA with the names, addresses, credit card numbers, and travel itineraries of persons who had flown on Northwest Airlines between July and December 2001.

The discovery of Northwest Airlines' disclosure of its customers' personal information triggered a wave of litigation. Eight class actions — seven in Minnesota and one in Tennessee — were filed in federal court prior to March 19, 2004. The seven Minnesota actions were later consolidated into a master file.

[In this case, t]he complaint alleges that Northwest Airlines' unauthorized disclosure of customers' personal information constituted a violation of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2702(a)(1) and (a)(3). . . .

---

[81] *Id.* at 831.

The Electronic Communications Privacy Act (ECPA) provides in relevant part that, with certain exceptions, a person or entity providing either an electronic communication service or remote computing service to the public shall not:

- knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service (18 U.S.C. § 2702(a)(1)); and
- knowingly divulge a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity (18 U.S.C. § 2702(a)(3)).

In its complaint, the Plaintiffs asserted claims under both 18 U.S.C. §§ 2702(a)(1) and (a)(3) of the ECPA. The plaintiffs have conceded no claim exists under 18 U.S.C. § 2702(a)(1). Consequently, the Court's focus will be directed at the Plaintiffs' ability to sustain a claim against Northwest Airlines under 18 U.S.C. § 2702(a)(3). To sustain a claim under 18 U.S.C. § 2702(a)(3), the Plaintiffs must establish that Northwest Airlines provides either electronic communication services or remote computing services. It is clear that Northwest Airlines provides neither.

The ECPA defines "electronic communication service" as "any service which provides the users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). In construing this definition, courts have distinguished those entities that sell access to the internet from those that sell goods or services on the internet. 18 U.S.C. § 2702(a)(3) prescribes the conduct only of a "provider of a remote computing service or electronic communication service to the public." A provider under the ECPA is commonly referred to as an internet service provider or ISP. There is no factual allegation that Northwest Airlines, an airline that sells airline tickets on its website, provides internet services.

Courts have concluded that "electronic communication service" encompasses internet service providers as well as telecommunications companies whose lines carry internet traffic, but does not encompass businesses selling traditional products or services online. See *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001). . . .

The distinction is critical in this case. Northwest Airlines is not an electronic communications service provider as contemplated by the ECPA. Instead, Northwest Airlines sells its products and services over the internet as opposed to access to the internet itself. The ECPA definition of "electronic communications service" clearly includes internet service providers such as America Online, as well as telecommunications companies whose cables and phone lines carry internet traffic. However, businesses offering their traditional products and services online through a website are not providing an "electronic communication service." As a result, Northwest Airlines falls outside the scope of 18 U.S.C. § 2702 and the ECPA claim fails as a matter of law. The facts as pled do not give rise to liability under the ECPA. 18 U.S.C. § 2702(a) does not prohibit or even address the dissemination of business records of passenger flights and information as described in the complaint. Instead, the focus of 18 U.S.C. § 2702(a) is on "communications" being stored by the communications service provider for the purpose of subsequent transmission or for backup purposes.

[The plaintiffs also raised a claim under the Minnesota Deceptive Trade Practices Act. The court held that the claim was barred by the federal Airline Deregulation Act, which preempts state regulation of "a price, route, or service of an airline carrier." 49 U.S.C. § 4173(b)(1).]

NOTES & QUESTIONS

1. ***ISPs vs. Non-ISPs.*** In this case, Northwest Airlines violated its privacy policy by disclosing its customer records to the government. Suppose Northwest Airlines had been an ISP like AOL or Earthlink. Would it have been liable under the Stored Communications Act?
2. ***Other Remedies.*** What other potential remedies might the plaintiffs have in this case? The plaintiffs brought an action for breach of contract, which was discussed earlier in this chapter in the section on privacy policies. Besides breach of contract, can you think of any other causes of action that might be brought?

(c) The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) of 1984, 18 U.S.C. § 1030, provides criminal and civil penalties for unauthorized access to computers. Originally passed in 1984, the statue was amended updated throughout the 1990s. Several states have similar statutes regarding the misuse of computers. As Orin Kerr notes:

> While no two statutes are identical, all share the common trigger of "access without authorization" or "unauthorized access" to computers, sometimes in tandem with its close cousin, "exceeding authorized access" to computers.[82]

Scope. The CFAA applies to all "protected computer[s]." A "protected computer" is any computer used in interstate commerce or communication. Whereas the Stored Communications Act of ECPA appears to apply only to ISPs, the CFAA applies to both ISPs and individual computers.

Criminal Penalties. The CFAA creates seven crimes. Among these, it imposes criminal penalties when a person or entity "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." § 1030(a)(2)(c). It criminalizes unauthorized access to "any nonpublic computer of a department or agency of the United States." § 1030(a)(3). The CFAA also criminalizes unauthorized access to computers "knowingly with intent to defraud" and the obtaining of "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." § 1030(a)(4). Yet another crime created by the CFAA prohibits knowingly transmitting "a program, information, code, or command" or "intentionally access[ing] a protected computer without authorization" that causes damage to a

[82] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1615 (2003).

protected computer. § 1030(5)(A)(i). Punishments range from fines to imprisonment for up to 20 years depending upon the provision violated.

Damage. The term "damage" means "any impairment to the integrity or availability of data, a program, a system, or information." § 1030(e). In many provisions in the CFAA, the damage must exceed $5,000 in a one-year period.

Civil Remedies. "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages or injunctive relief or other equitable relief." § 1030(g). "Damage" must cause a "loss aggregating at least $5,000 in value during any 1-year period to one or more individuals." § 1030(e).

Exceeding Authorized Access. Many provisions in the CFAA can be violated not just by unauthorized access, but also when one "exceeds authorized access." To exceed authorized access means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain and alter." § 1030(e)(6).

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. "Dead heading" 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 loadmatching 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."[83] The new version, in effect now and during trial, says "loss . . . during any 1-year period . . . aggregating at least $5,000 in value."[84] 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."

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

[83] 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.").

[84] 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.").

"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." The damage floor in the Computer Fraud and Abuse Act contains no "single act" requirement.

NOTES & QUESTIONS

1. ***The $5,000 Threshold.*** In *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001), the plaintiffs brought a CFAA claim and contended that collectively they suffered more than $5,000 in damages. But the court held that the plaintiffs could not add up their damages. Damages could only be combined "for a single act" against "a particular computer." Since the plaintiffs' CFAA claims concerned multiple acts against many different computers, they could not be aggregated to reach the $5,000 threshold.
2. ***Spyware.*** Spyware is a new kind of computer program that raises significant threats to privacy. Paul Schwartz distinguishes "spyware" from "adware" in terms of the notice provided to the user. He also explains how these programs come about through the linking of personal computers via the Internet: "Spyware draws on computer resources to create a network that can be used for numerous purposes, including collecting personal and nonpersonal information from computers and delivering adware or targeted advertisements to individuals surfing the Web. Adware is sometimes, but not always, delivered as part of spyware; the definitional line between the two depends on whether the computer user receives adequate notice of the program's installation."[85] Would the CFAA apply to a company that secretly installs spyware in a person's computer that transmits her personal data back to the company without her awareness? Would the Wiretap Act apply?
3. ***State Spyware Statutes.*** The state of Utah became the first state to pass legislation to regulate spyware. The original Spyware Control Act, Utah Code Ann. §§ 13-40-101 *et seq.*, prohibited the installation of spyware on another person's computer, limited the display of certain types of advertising, created a private right of action, and empowered the Utah Division of Consumer Protection to collect complaints. WhenU, an advertising network, challenged the Act in 2004, arguing that it violated the Commerce Clause of the U.S. Constitution, and it obtained a preliminary injunction against the statute. A revised bill was signed by the Utah governor on March 17, 2005. The revised Act defines "spyware" as "software on a computer of a user who resides in this state that . . . collects information about an Internet website at the time the

[85] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055 (2004).

Internet website is being viewed in this state, unless the Internet website is the Internet website of the person who provides the software; and . . . uses the information . . . contemporaneously to display pop-up advertising on the computer."

Following Utah's lead, California enacted a spyware bill, which was signed by Governor Arnold Schwarzenegger on September 28, 2004. The Consumer Protection Against Computer Spyware Act, SB 1426, prohibits a person from causing computer software to be installed on a computer and using the software to (1) take control of the computer; (2) modify certain settings relating to the computer's access to the Internet; (3) collect, through intentionally deceptive means, personally identifiable information; (4) prevent, without authorization, the authorized user's reasonable efforts to block the installation of or disable software; (5) intentionally misrepresent that the software will be uninstalled or disabled by the authorized user's action; or (6) through intentionally deceptive means, remove, disable, or render, inoperative security, anti-spyware, or antivirus software installed on the computer.

UNITED STATES V. DREW

259 F.R.D. 449 (C.D. Cal. 2009)

WU, J. This case raises the issue of whether (and/or when will) violations of an Internet website's terms of service constitute a crime under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. . . .

In the Indictment, Drew was charged with one count of conspiracy in violation of 18 U.S.C. § 371 and three counts of violating a felony portion of the CFAA, *i.e.,* 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), which prohibit accessing a computer without authorization or in excess of authorization and obtaining information from a protected computer where the conduct involves an interstate or foreign communication and the offense is committed in furtherance of a crime or tortious act.

The Indictment included, *inter alia,* the following allegations (not all of which were established by the evidence at trial). Drew, a resident of O'Fallon, Missouri, entered into a conspiracy in which its members agreed to intentionally access a computer used in interstate commerce without (and/or in excess of) authorization in order to obtain information for the purpose of committing the tortious act of intentional infliction of emotional distress upon "M.T.M.," subsequently identified as Megan Meier ("Megan"). Megan was a 13 year old girl living in O'Fallon who had been a classmate of Drew's daughter Sarah. Pursuant to the conspiracy, on or about September 20, 2006, the conspirators registered and set up a profile for a fictitious 16 year old male juvenile named "Josh Evans" on the www. My Space. com website ("MySpace"), and posted a photograph of a boy without that boy's knowledge or consent. Such conduct violated My Space's terms of service. The conspirators contacted Megan through the MySpace network (on which she had her own profile) using the Josh Evans pseudonym and began to flirt with her over a number of days. On or about October 7, 2006, the conspirators had "Josh" inform Megan that he was moving away. On or about October 16, 2006, the conspirators had "Josh" tell Megan that he no longer liked her and that "the world would be a better place without her in it." Later on that same day, after learning that Megan had killed herself, Drew caused the Josh Evans MySpace account to be deleted.

At the trial, after consultation between counsel and the Court, the jury was instructed that, if they unanimously decided that they were not convinced beyond a reasonable doubt as to the Defendant's guilt as to the felony CFAA violations of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), they could then consider whether the Defendant was guilty of the "lesser included" misdemeanor CFAA violation of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A). [The jury found Drew not guilty of the felony CFAA violations and guilty of the misdemeanor CFAA violation. Drew made a motion for judgment of acquittal under Fed. R. Crim. P. 29(c).]

As Jae Sung (Vice President of Customer Care at MySpace) testified at trial, MySpace is a "social networking" website where members can create "profiles" and interact with other members. . . .

In 2006, to become a member, one had to go to the sign-up section of the MySpace website and register by filling in personal information (such as name, email address, date of birth, country/state/postal code, and gender) and creating a password. In addition, the individual had to check on the box indicating that "You agree to the MySpace Terms of Service and Privacy Policy." The terms of service did not appear on the same registration page that contained this "check box" for users to confirm their agreement to those provisions. . . . A person could become a MySpace member without ever reading or otherwise becoming aware of the provisions and conditions of the MySpace terms of service [MSTOS] by merely clicking on the "check box" and then the "Sign Up" button without first accessing the "Terms" section.

The MSTOS prohibited the posting of a wide range of content on the website including (but not limited to) material that: a) "is potentially offensive and promotes racism, bigotry, hatred or physical harm of any kind against any group or individual"; b) "harasses or advocates harassment of another person"; c) "solicits personal information from anyone under 18"; d) "provides information that you know is false or misleading or promotes illegal activities or conduct that is abusive, threatening, obscene, defamatory or libelous"; e) "includes a photograph of another person that you have posted without that person's consent"; f) "involves commercial activities and/or sales without our prior written consent"; g) "contains restricted or password only access pages or hidden pages or images"; or h) "provides any phone numbers, street addresses, last names, URLs or email addresses. . . ."

[In 2006, the CFAA (18 U.S.C. § 1030) punished a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."]

As used in the CFAA, the term "computer" "includes any data storage facility or communication facility directly related to or operating in conjunction with such device. . . ." 18 U.S.C. § 1030(e)(1). The term "protected computer" "means a computer—(A) exclusively for the use of a financial institution or the United States Government . . . ; or (B) which is used in interstate or foreign commerce or communication. . . ." *Id.* § 1030(e)(2). The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain

or alter information in the computer that the accesser is not entitled so to obtain or alter . . . ." *Id.* § 1030(e)(6).

In addition to providing criminal penalties for computer fraud and abuse, the CFAA also states that "[A]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g). Because of the availability of civil remedies, much of the law as to the meaning and scope of the CFAA has been developed in the context of civil cases.

During the relevant time period herein, the misdemeanor 18 U.S.C. § 1030(a)(2)(C) crime consisted of the following three elements:

First, the defendant intentionally [accessed without authorization] [exceeded authorized access of] a computer;

Second, the defendant's access of the computer involved an interstate or foreign communication; and

Third, by [accessing without authorization] [exceeding authorized access to] a computer, the defendant obtained information from a computer . . . [used in interstate or foreign commerce or communication] . . . .

As to the term "without authorization," the courts that have considered the phrase have taken a number of different approaches in their analysis. . . . [W]here the relationship between the parties is contractual in nature or resembles such a relationship, access has been held to be unauthorized where there has been an ostensible breach of contract. . . .

Within the breach of contract approach, most courts that have considered the issue have held that a conscious violation of a website's terms of service/use will render the access unauthorized and/or cause it to exceed authorization. *See, e.g., Southwest Airlines Co. v. Farechase, Inc.,* 318 F. Supp. 2d 435, 439-40 (N.D. Tex. 2004); *Nat'l Health Care Disc., Inc.,* 174 F. Supp. 2d at 899; *Register.com, Inc. v. Verio, Inc.,* 126 F. Supp. 2d 238, 247-51 (S.D.N.Y. 2000), *aff'd,* 356 F.3d 393 (2d Cir. 2004); *Am. Online, Inc. v. LCGM, Inc.,* 46 F. Supp. 2d 444, 450 (E.D. Va. 1998); *see also EF Cultural Travel BV v. Zefer Corp.,* 318 F.3d 58, 62-63 (1st Cir. 2003) ("A lack of authorization could be established by an explicit statement on the website restricting access. . . . [W]e think that the public website provider can easily spell out explicitly what is forbidden. . . ."). . . .

In this particular case, as conceded by the Government, the only basis for finding that Drew intentionally accessed MySpace's computer/servers without authorization and/or in excess of authorization was her and/or her co-conspirator's violations of the MSTOS by deliberately creating the false Josh Evans profile, posting a photograph of a juvenile without his permission and pretending to be a sixteen year old O'Fallon resident for the purpose of communicating with Megan. Therefore, if conscious violations of the My Space terms of service were not sufficient to satisfy the first element of the CFAA misdemeanor violation as per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(b)(2)(A), Drew's Rule 29(c) motion would have to be granted on that basis alone. However, this Court concludes that an intentional breach of the MSTOS can potentially constitute accessing the MySpace computer/server without authorization and/or in excess of authorization under the statute. . . .

Justice Holmes observed that, as to criminal statutes, there is a "fair warning" requirement. . . .

The void-for-vagueness doctrine has two prongs: 1) a definitional/notice sufficiency requirement and, more importantly, 2) a guideline setting element to govern law enforcement. In *Kolender v. Lawson,* 461 U.S. 352 (1983), the Court explained that:

> As generally stated, the void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement. . . .

To avoid contravening the void-for-vagueness doctrine, the criminal statute must contain "relatively clear guidelines as to prohibited conduct" and provide "objective criteria" to evaluate whether a crime has been committed. . . .

The pivotal issue herein is whether basing a CFAA misdemeanor violation as per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A) upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine. This Court concludes that it does primarily because of the absence of minimal guidelines to govern law enforcement, but also because of actual notice deficiencies. . . .

First, an initial inquiry is whether the statute, as it is written, provides sufficient notice. Here, the language of section 1030(a)(2)(C) does not explicitly state (nor does it implicitly suggest) that the CFAA has "criminalized breaches of contract" in the context of website terms of service. Normally, breaches of contract are not the subject of criminal prosecution. Thus, while "ordinary people" might expect to be exposed to civil liabilities for violating a contractual provision, they would not expect criminal penalties. . . .

Second, if a website's terms of service controls what is "authorized" and what is "exceeding authorization" — which in turn governs whether an individual's accessing information or services on the website is criminal or not, section 1030(a)(2)(C) would be unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will. . . .

Third, by utilizing violations of the terms of service as the basis for the section 1030(a)(2)(C) crime, that approach makes the website owner — in essence — the party who ultimately defines the criminal conduct. This will lead to further vagueness problems. The owner's description of a term of service might itself be so vague as to make the visitor or member reasonably unsure of what the term of service covers. . . .

Fourth, because terms of service are essentially a contractual means for setting the scope of authorized access, a level of indefiniteness arises from the necessary application of contract law in general and/or other contractual requirements within the applicable terms of service to any criminal prosecution. . . .

Treating a violation of a website's terms of service, without more, to be sufficient to constitute "intentionally access[ing] a computer without authorization or exceed[ing] authorized access" would result in transforming section 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals. . . .

One need only look to the MSTOS terms of service to see the expansive and elaborate scope of such provisions whose breach engenders the potential for

criminal prosecution. Obvious examples of such breadth would include: 1) the lonely-heart who submits intentionally inaccurate data about his or her age, height and/or physical appearance, which contravenes the MSTOS prohibition against providing "information that you know is false or misleading"; 2) the student who posts candid photographs of classmates without their permission, which breaches the MSTOS provision covering "a photograph of another person that you have posted without that person's consent"; and/or 3) the exasperated parent who sends out a group message to neighborhood friends entreating them to purchase his or her daughter's girl scout cookies, which transgresses the MSTOS rule against "advertising to, or solicitation of, any Member to buy or sell any products or services through the Services." However, one need not consider hypotheticals to demonstrate the problem. In this case, Megan (who was then 13 years old) had her own profile on MySpace, which was in clear violation of the MSTOS which requires that users be "14 years of age or older." No one would seriously suggest that Megan's conduct was criminal or should be subject to criminal prosecution. . . .

In sum, if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law "that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]."

NOTES & QUESTIONS

1. ***The Implications of* Drew.** Is the prosecutor's theory consistent with the CFAA's purpose? Suppose the court in *Drew* had reached the opposite conclusion. What effect would criminal liability for violating a website's terms of service have for people who use the Internet?
2. ***Is the CFAA Unconstitutionally Vague?*** The *Drew* court's holding is narrow, concluding only that the application of the CFAA to website terms of service violations would be unconstitutionally vague. More broadly, is the CFAA unconstitutionally vague on its face?

3. MARKETING

(a) The Telephone Consumer Protections Act

The Telephone Consumer Protections Act (TCPA) of 1991, Pub. L. No. 102-243, 47 U.S.C. § 227, requires the FCC to promulgate rules to "protect residential telephone subscribers' privacy rights and to avoid receiving telephone solicitations to which they object." § 227(c)(1). In addition, the FCC is authorized to require that a "single national database" be established of a "list of telephone numbers of residential subscribers who object to receiving telephone solicitations." § 227(c)(3).

Private Right of Action. The FCPA provides plaintiffs with a private right of action in small claims court against an entity for each call received after requesting

to no longer receive calls from that entity. Plaintiffs can sue for an actual loss or up to $500 (whichever is greater), If telemarketer has acted "willfully or knowingly," then damages are trebled. § 227(c)(5).

Affirmative Defense. Telemarketers can offer as an affirmative defense that they established "reasonable practices and procedures to effectively prevent telephone solicitations in violation of the regulations prescribed under this subsection." § 227(c)(5).

Prohibition on Using Pre-Recorded Messages. The TCPA prohibits telemarketers from calling residences and using prerecorded messages without the consent of the called party. 47 U.S.C. § 227(b)(1)(B).

Fax Machines. The TCPA prohibits the use of a fax, computer, or other device to send an unsolicited advertisement to a fax machine. § 227(b)(1)(C).

State Enforcement. States may initiate actions against telemarketers "engaging in a pattern or practice of telephone calls or other transmissions to residents of that State" in violation of the TCPA. § 227(f)(1).

NOTES & QUESTIONS

1. ***First Amendment Limitations?*** In *Destination Ventures, Ltd. v. FCC,* 46 F.3d 54 (9th Cir. 1995), Destination Ventures challenged a provision of the TCPA banning unsolicited faxes that contained advertisements on First Amendment grounds. The court upheld the ban because it was designed to prevent shifting advertising costs to consumers, who would be forced to pay for the toner and paper to receive the ads.
2. ***A Do Not Track List.*** As a continuation of the "Do Not Call" list, a discussion is now emerging about "Do Not Track" (DNT) protection for the Internet. The idea of DNT turns on the use of an "opt-out header" in a Web browser.[86] The FTC has told Congress that it supports giving consumers a DNT option to give them a simple and easy way to control the fashion in which companies track them online.

   In contrast to "Do Not Call," considerable complexity exists around the concept of "tracking" on the Internet. The Center for Democracy and Technology (CDT) has defined tracking "as the collection and correlation of data about the Internet activities of a particular user, computer or device, over time and across non-commonly branded websites, for any purpose other than fraud prevention or compliance with law enforcement requests."[87] Thus, CDT considers behavioral advertising as "tracking."

---

[86] For more on the technology behind this policy proposal, see *Do Not Track*, at http://www.donottrack.us/.

[87] CDT, *What Does "Do Not Track" Mean?* (Jan. 31, 2011). For an approach that is largely in agreement with the CDT, see Electronic Frontier Foundation, *What Does the "Track" in "Do Not Track" Mean?* (Feb. 19, 2011).

CDT also argues that any "actively shared" data, such as information that data users provide in social networking profiles and Web forums or by registering for various accounts, should not fall within Do Not Track prohibitions.

Consider Omer Tene and Jules Polonetsky:

> The FTC put forth the following criteria to assess industry responses: DNT should be universal, that is, a single opt-out should cover all would-be trackers; easy to find, understand, and use; persistent, meaning that opt-out choices do not "vanish"; effective and enforceable, covering all tracking technologies; and controlling not only use of data but also their collection.[88] As discussed, the FTC has not yet taken a position on whether any legislation or rulemaking is necessary for DNT. It is clear, however, that regardless of the regulatory approach chosen, industry collaboration will remain key since the system will only work if websites and ad intermediaries respect users' preferences. . . .
>
> The debate raging around online behavioral tracking generally and DNT in particular is a smoke screen for a discussion that all parties hesitate to hold around deeper values and social norms. Which is more important — efficiency or privacy; law enforcement or individual rights; reputation or freedom of speech? Policymakers must engage with the underlying normative question: is online behavioral tracking a societal good, funding the virtue of the online economy and bringing users more relevant, personalized content and services; or is it an evil scheme for businesses to enrich themselves on account of ignorant users and for governments to create a foundation for pervasive surveillance? Policymakers cannot continue to sidestep these questions in the hope that "users will decide" for themselves.[89]

3. ***Revocation of Consent.*** In *Gager v. Dell Financial Services*, 727 F.3d 265 (3d Cir. 2013), the plaintiff applied for a credit line from Dell to purchase computer equipment. She listed her cell phone number. Dell began calling her cell phone using an automated telephone dialing system. The plaintiff wrote a letter to Dell requesting that it stop calling. Dell continued its calls, calling about 40 times over a three-week span. The plaintiff brought a TCPA action. Dell moved to dismiss claiming that the FTCPA did not provide a way for people to revoke prior consent. The court, however, concluded that "the absence of an express statutory authorization for revocation of prior express consent in the TCPA's provisions on autodialed calls to cellular phones does not tip the scales in favor of a position that no such right exists." The court reasoned that "the common law concept of consent shows that it is revocable" and that "in light of the TCPA's purpose, any silence in the statute as to the right of revocation should be construed in favor of consumers."

[88] Ed Felten, FTC Perspective, W3C Workshop on Web Tracking and User Privacy, Apr. 28-29, 2011, http://www.w3.org/2011/track-privacy/slides/Felten.pdf.

[89] Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, available at http://www.futureofprivacy.org/tracking/.

(b) The CAN-SPAM Act

In 2003, Congress enacted the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, Pub. L. No. 108-187, 15 U.S.C. §§ 7701 *et seq.*, to address the problem of spam. Spam is a term to describe unsolicited commercial e-mail sent to individuals to advertise products and services.[90] Companies that send unsolicited e-mail are referred to as spammers. Spam is often mailed out in bulk to large lists of e-mail addresses. A recent practice has been to insert hidden HTML tags (also known as "pixel tags" or "Web bugs") into spam. This enables the sender of the e-mail to detect whether the e-mail was opened. It can also inform the sender about whether the e-mail message was forwarded, to what e-mail address it was forwarded, and sometimes, even comments added by a user when forwarding the e-mail. This only works if the recipient has an HTML-enabled e-mail reader rather than a text-only reader. HTML e-mail is e-mail that contains pictures and images rather than simply plain text.

Applicability. The CAN-SPAM Act applies to commercial e-mail, which it defines as a "message with the primary purpose of which is the commercial advertisement or promotion of a commercial product or service."

Prohibitions. The Act prohibits the knowing sending of commercial messages with the intent to deceive or mislead recipients.

Opt Out. The CAN-SPAM Act also requires that a valid opt-out option be made available to e-mail recipients. To make opt out possible, the Act requires senders of commercial e-mail to contain a return address "clearly and conspicuously displayed." Finally, it creates civil and criminal penalties for violations of its provisions. For example, the law allows the DOJ to seek criminal penalties, including imprisonment, for commercial e-mailers who engage in activities such as using a computer to relay or retransmit multiple commercial e-mail messages to receive or mislead recipients or an Internet access service about the message's origin and falsifying header information in multiple e-mail messages and initiate the transmission of these messages.

Enforcement. The CAN-SPAM Act is enforced by governmental and private entities. The chief enforcement entities are the Department of Justice (DOJ), the Federal Trade Commission (FTC), state attorney generals, and "Internet access services" (IAS). Unlike similar laws in other countries, such as Canada's Anti-Spam Legislation (CASL), the CAN-SPAM Act lacks a general private right of action.

The DOJ is charged with enforcing the Act's criminal provisions. These prohibit the unlawful transmission of sexually oriented unsolicited commercial e-mail as well as certain methods of sending commercial e-mail, such as zombie drones, materially false header information, and obtaining IP addresses through

[90] For more information on spam, see David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. Rev. 325, 336 (2001).

fraudulent methods. The FTC and state attorney generals also have an enforcement role under the CAN-SPAM Act. The FTC has been involved both in litigation and settlement actions.

Finally, an IAS that has been adversely affected by violations of the CAN-SPAM Act has standing under the statute. The Act defines an IAS as "a service that enables users to access content, information, electronic mail, or other services over the Internet. . ." 47 U.S.C. § 231(e)(4) . Courts have found Internet Service Providers, social networking websites, and email providers to be an IAS.

Assessing the Act. A year after enactment of CAN-SPAM, media accounts faulted the law as ineffective. Indeed, reports stressed the increase in spam during this time. According to one anti-spam vendor, 67 percent of all e-mail was spam in February 2004, and 75 percent in November 2004. Some spammers employed new tactics after the passage of the Act, such as using "zombie networks," which involve hijacking computers with Trojan horse programs. Anti-spam activists faulted CAN-SPAM for preempting tougher state laws, failing to provide a general private right of action, and providing an opt-out option instead of an opt in.[91]

State Anti-Spam Laws. At least 20 states have anti-spam statutes. For example, Cal. Bus. & Professions Code § 17538.4 mandates that senders of spam include in the text of their e-mails a way through which recipients can request to receive no further e-mails. The sender must remove the person from its list. A provider of an e-mail service located within the state of California can request that spammers stop sending spam through its equipment. If the spammer continues to send e-mail, it can be liable for $50 per message up to a maximum of $25,000 per day. *See* § 17538.45.

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."[92] 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?

[91] For a range of reform proposals, see David Lorentz, *Note: The Effectiveness of Litigation Under the CAN-SPAM Act*, 30 Rev. Litig. 559 (2011).

Spam and Speech. Is spam a form of speech, protected by the First Amendment? In *Cyber Promotions, Inc. v. America Online, Inc.,* 948 F. Supp. 436 (E.D. Pa. 1996), Cyber Promotions, Inc. sought a declaratory judgment that America Online (AOL) was prohibited under the First Amendment from denying it the ability to send AOL customers unsolicited e-mail. The court rejected Cyber Promotion's argument because of a lack of state action: "AOL is a private online company that is not owned in whole or part by the government." Today, the Internet is increasingly becoming a major medium of communication. Prior to modern communications media, individuals could express their views in traditional "public fora" — parks and street corners. These public fora are no longer the central place for public discourse. Perhaps the Internet is the modern public forum, the place where individuals come to speak and express their views. If this is the case, is it preferable for access to the Internet to be controlled by private entities?

International Approaches. Unlike the CAN-SPAM in the United States, most other countries favor an opt-in approach as a legal response to commercial unsolicited emails. For example, CASL in Canada generally permits the sending of commercial email only when there is consent.[93] CASL provides for strong administrative penalties as well as a private right of action.

This preference for an opt-in regime is also found in Australia's Spam Act of 2003 and New Zealand's Unsolicited Electronic Messages Act of 2007. In the European Union, the E-Privacy Directive, first enacted in 2002 and amended in 2009, states that the use of "electronic mail for the purposes of direct marketing may be only allowed in respect of subscribers who have given their prior consent."[94]

Within the EU, Germany is the country that may have the strictest regulation of spam. Its main provision prohibiting spam is Article 7 of the Act against Unfair Competition (UWG). This clause prohibits the sending of advertising emails that constitute an "unconscionable pestering." Clause 7(2) no.3 of this statute contains the critical language; it forbids advertising through email without "prior express consent" of the recipient. In German law, prior express consent requires a process termed "double opt-in." For example, a consumer might agree to receive commercial emails by checking a box, confirming the selection, and then opt-in

[92] Eric Goldman, *A Cosean Analysis of Marketing*, 2006 Wis. L. Rev. 1151, 1154-55, 1202, 1211-12.

[93] Bill C-28, Fighting Internet and Wireless Spam Act, 3rd Session, 40th Parl., 2010.

[94] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), L201, 2002-07-31, pp. 37-47 (2002); Directive 2009/136/EC of the European Parliament and of the Council of 25. November 2009, L337, 2009-12-18, pp. 11-36 (2009).

again by clicking on a link contained in the first email that she received after enrollment.[95]

Would an opt-in system be preferable to the current U.S. approach? Would there be benefits for the U.S. switching to opt-in to make regulations in this area of law more uniform internationally?

G. FIRST AMENDMENT LIMITATIONS ON PRIVACY REGULATION

Although the First Amendment protects privacy, privacy restrictions can come into conflict with the First Amendment. In particular, many privacy statutes regulate the disclosure of true information. The cases in this section explore the extent to which the First Amendment limits the privacy statutes. Before turning to the cases, some background about basic First Amendment jurisprudence is necessary. The cases in this section often focus on commercial speech, and the Court analyzes commercial speech differently than other forms of expression.

First Amendment Protection of Commercial Speech. For a while, the Court considered commercial speech as a category of expression that is not accorded First Amendment protection. However, in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.,* 425 U.S. 748 (1976), the Court held that commercial speech deserves constitutional protection. However, the Court held that commercial speech has a lower value than regular categories of speech and therefore is entitled to a lesser protection. *Ohralik v. Ohio State Bar Ass'n,* 436 U.S. 447 (1978).

Defining Commercial Speech. What is "commercial speech"? The Court has defined it as speech that "proposes a commercial transaction," *Virginia State Board,* 425 U.S. 748 (1976), and as "expression related solely to the economic interests of the speaker and its audience." *Central Hudson Gas & Electric Corp. v. Public Service Comm'n of New York,* 447 U.S. 557 (1980). The Court later held that neither of these are necessary requirements to define commercial speech; both are factors to be considered in determining whether speech is commercial. *See Bolger v. Youngs Drug Products Corp.,* 463 U.S. 60 (1983).

The* Central Hudson *Test. In *Central Hudson,* 447 U.S. 557 (1980), the Court established a four-part test for analyzing the constitutionality of restrictions on commercial speech:

> At the outset, we must determine whether the expression is protected by the First Amendment. For commercial speech to come within that provision, it at least must concern lawful activity and not be misleading. Next, we ask whether the asserted governmental interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.

[95] For German caselaw finding a requirement of double-opt in, see AG Düsseldorf, Decision of July 14, 2009 - 48 C 1911/09, BeckRS 2009, 25861; LG Essen, Decision of April 20, 2009 - 4 O 368/08, NJW-RR 2009, 1556; OLG Hamm, Decision of February 17, 2011 - I-4 U 174/10 (LG Dortmund) (rechtskräftig), MMR 2011, 539; OLG Jena, Decision of April 21, 2010 – 2 U 88/10, NJOZ 2011, 1164.

In *Board of Trustees of State University of New York v. Fox,* 492 U.S. 469 (1989), the Court revised the last part of the *Central Hudson* test — that speech "not [be] more extensive than is necessary to serve [the governmental] interest" — to a requirement that there be a "fit between the legislature's ends and the means chosen to accomplish the ends, . . . a fit that is not necessarily perfect, but reasonable."

In *Cincinnati v. Discovery Network, Inc.,* 507 U.S. 410 (1993), the Court, applying the commercial speech test in *Central Hudson* and *Fox*, struck down an ordinance that banned newsracks with "commercial handbills." The ordinance did not apply to newsracks for newspapers. The Court concluded that the ban was not a "reasonable fit" with the city's interest in aesthetics. Moreover, the Court concluded that the ordinance was not content-neutral. The Court held that Cincinnati "has enacted a sweeping ban on the use of newsracks that distribute 'commercial handbills,' but not 'newspapers.' Under the city's newsrack policy, whether any particular newsrack falls within the ban is determined by the content of the publication resting inside that newsrack. Thus, by any commonsense understanding of the term, the ban in this case is 'content based.' . . . [B]ecause the ban is predicated on the content of the publications distributed by the subject newsracks, it is not a valid time, place, or manner restriction on protected speech."

ROWAN V. UNITED STATES POST OFFICE DEPARTMENT

397 U.S. 728 (1970)

[A federal statute permitted individuals to require that entities sending unwanted mailings remove the individuals' names from their mailing lists and cease to send future mailings. A group of organizations challenged the statute on First Amendment grounds.]

BURGER, C.J. . . . The essence of appellants' argument is that the statute violates their constitutional right to communicate. . . . Without doubt the public postal system is an indispensable adjunct of every civilized society and communication is imperative to a healthy social order. But the right of every person "to be let alone" must be placed in the scales with the right of others to communicate.

In today's complex society we are inescapably captive audiences for many purposes, but a sufficient measure of individual autonomy must survive to permit every householder to exercise control over unwanted mail. To make the householder the exclusive and final judge of what will cross his threshold undoubtedly has the effect of impeding the flow of ideas, information, and arguments that, ideally, he should receive and consider. Today's merchandising methods, the plethora of mass mailings subsidized by low postal rates, and the growth of the

sale of large mailing lists as an industry in itself have changed the mailman from a carrier of primarily private communications, as he was in a more leisurely day, and have made him an adjunct of the mass mailer who sends unsolicited and often unwanted mail into every home. It places no strain on the doctrine of judicial notice to observe that whether measured by pieces or pounds, Everyman's mail today is made up overwhelmingly of material he did not seek from persons he does not know. And all too often it is matter he finds offensive. . . .

The Court has traditionally respected the right of a householder to bar, by order or notice, solicitors, hawkers, and peddlers from his property. In this case the mailer's right to communicate is circumscribed only by an affirmative act of the addressee giving notice that he wishes no further mailings from that mailer.

To hold less would tend to license a form of trespass and would make hardly more sense than to say that a radio or television viewer may not twist the dial to cut off an offensive or boring communication and thus bar its entering his home. Nothing in the Constitution compels us to listen to or view any unwanted communication, whatever its merit; we see no basis for according the printed word or pictures a different or more preferred status because they are sent by mail. The ancient concept that "a man's home is his castle" into which "not even the king may enter" has lost none of its vitality, and none of the recognized exceptions includes any right to communicate offensively with another. . . .

If this prohibition operates to impede the flow of even valid ideas, the answer is that no one has a right to press even "good" ideas on an unwilling recipient. That we are often "captives" outside the sanctuary of the home and subject to objectionable speech and other sound does not mean we must be captives everywhere. The asserted right of a mailer, we repeat, stops at the outer boundary of every person's domain. . . .

MAINSTREAM MARKETING SERVICES, INC. V. FEDERAL TRADE COMMISSION

358 F.3d 1228 (10th Cir. 2004)

EBEL, J. . . . In 2003, two federal agencies—the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) — promulgated rules that together created the national do-not-call registry *See* 16 C.F.R. § 310.4(b)(1)(iii)(B) (FTC rule); 47 C.F.R. § 64.1200(c)(2) (FCC rule). The national do-not-call registry is a list containing the personal telephone numbers of telephone subscribers who have voluntarily indicated that they do not wish to receive unsolicited calls from commercial telemarketers. Commercial telemarketers are generally prohibited from calling phone numbers that have been placed on the do-not-call registry, and they must pay an annual fee to access the numbers on the registry so that they can delete those numbers from their telephone solicitation lists. So far, consumers have registered more than 50 million phone numbers on the national do-not-call registry.

The national do-not-call registry's restrictions apply only to telemarketing calls made by or on behalf of sellers of goods or services, and not to charitable or political fundraising calls. Additionally, a seller may call consumers who have signed up for the national registry if it has an established business relationship with the consumer or if the consumer has given that seller express written permission

to call. Telemarketers generally have three months from the date on which a consumer signs up for the registry to remove the consumer's phone number from their call lists. Consumer registrations remain valid for five years, and phone numbers that are disconnected or reassigned will be periodically removed from the registry.

The national do-not-call registry is the product of a regulatory effort dating back to 1991 aimed at protecting the privacy rights of consumers and curbing the risk of telemarketing abuse. In the Telephone Consumer Protection Act of 1991 ("TCPA") — under which the FCC enacted its do-not-call rules — Congress found that for many consumers telemarketing sales calls constitute an intrusive invasion of privacy. . . . The TCPA therefore authorized the FCC to establish a national database of consumers who object to receiving "telephone solicitations," which the act defined as commercial sales calls. . . .

The national do-not-call registry's telemarketing restrictions apply only to commercial speech. Like most commercial speech regulations, the do-not-call rules draw a line between commercial and non-commercial speech on the basis of content. In reviewing commercial speech regulations, we apply the *Central Hudson* test. *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.,* 447 U.S. 557 (1980).

Central Hudson established a three-part test governing First Amendment challenges to regulations restricting non-misleading commercial speech that relates to lawful activity. First, the government must assert a substantial interest to be achieved by the regulation. Second, the regulation must directly advance that governmental interest, meaning that it must do more than provide "only ineffective or remote support for the government's purpose." Third, although the regulation need not be the least restrictive measure available, it must be narrowly tailored not to restrict more speech than necessary. Together, these final two factors require that there be a reasonable fit between the government's objectives and the means it chooses to accomplish those ends. . . .

The government asserts that the do-not-call regulations are justified by its interests in 1) protecting the privacy of individuals in their homes, and 2) protecting consumers against the risk of fraudulent and abusive solicitation. Both of these justifications are undisputedly substantial governmental interests.

In *Rowan v. United States Post Office Dep't,* the Supreme Court upheld the right of a homeowner to restrict material that could be mailed to his or her house. The Court emphasized the importance of individual privacy, particularly in the context of the home, stating that "the ancient concept that 'a man's home is his castle' into which 'not even the king may enter' has lost none of its vitality." In *Frisby v. Schultz,* the Court [held] . . .

> One important aspect of residential privacy is protection of the unwilling listener. . . . [A] special benefit of the privacy all citizens enjoy within their own walls, which the State may legislate to protect, is an ability to avoid intrusions. Thus, we have repeatedly held that individuals are not required to welcome unwanted speech into their own homes and that the government may protect this freedom.

A reasonable fit exists between the do-not-call rules and the government's privacy and consumer protection interests if the regulation directly advances those interests and is narrowly tailored. . . .

These criteria are plainly established in this case. The do-not-call registry directly advances the government's interests by effectively blocking a significant number of the calls that cause the problems the government sought to redress. It is narrowly tailored because its opt-in character ensures that it does not inhibit any speech directed at the home of a willing listener.

The telemarketers assert that the do-not-call registry is unconstitutionally underinclusive because it does not apply to charitable and political callers. First Amendment challenges based on underinclusiveness face an uphill battle in the commercial speech context. As a general rule, the First Amendment does not require that the government regulate all aspects of a problem before it can make progress on any front. . . . The underinclusiveness of a commercial speech regulation is relevant only if it renders the regulatory framework so irrational that it fails materially to advance the aims that it was purportedly designed to further. . .

As discussed above, the national do-not-call registry is designed to reduce intrusions into personal privacy and the risk of telemarketing fraud and abuse that accompany unwanted telephone solicitation. The registry directly advances those goals. So far, more than 50 million telephone numbers have been registered on the do-not-call list, and the do-not-call regulations protect these households from receiving most unwanted telemarketing calls. According to the telemarketers' own estimate, 2.64 telemarketing calls per week — or more than 137 calls annually — were directed at an average consumer before the do-not-call list came into effect. *Cf.* 68 Fed. Reg. at 44152 (discussing the five-fold increase in the total number of telemarketing calls between 1991 and 2003). Accordingly, absent the do-not-call registry, telemarketers would call those consumers who have already signed up for the registry an estimated total of 6.85 *billion* times each year.

To be sure, the do-not-call list will not block all of these calls. Nevertheless, it will prohibit a substantial number of them, making it difficult to fathom how the registry could be called an "ineffective" means of stopping invasive or abusive calls, or a regulation that "furnish[es] only speculative or marginal support" for the government's interests. . . .

Finally, the type of unsolicited calls that the do-not-call list does prohibit—commercial sales calls — is the type that Congress, the FTC and the FCC have all determined to be most to blame for the problems the government is seeking to redress. According to the legislative history accompanying the TCPA, "[c]omplaint statistics show that unwanted commercial calls are a far bigger problem than unsolicited calls from political or charitable organizations." H.R. Rep. No. 102-317, at 16 (1991). Additionally, the FTC has found that commercial callers are more likely than non-commercial callers to engage in deceptive and abusive practices. . . . The speech regulated by the do-not-call list is therefore the speech most likely to cause the problems the government sought to alleviate in enacting that list, further demonstrating that the regulation directly advances the government's interests. . . .

Although the least restrictive means test is not the test to be used in the commercial speech context, commercial speech regulations do at least have to be "narrowly tailored" and provide a "reasonable fit" between the problem and the solution. Whether or not there are "numerous and obvious less-burdensome alternatives" is a relevant consideration in our narrow tailoring analysis. . . . We hold that the national do-not-call registry is narrowly tailored because it does not over-regulate protected speech; rather, it restricts only calls that are targeted at unwilling recipients. . . .

The Supreme Court has repeatedly held that speech restrictions based on private choice (i.e., an opt-in feature) are less restrictive than laws that prohibit speech directly. In *Rowan,* for example, the Court approved a law under which an individual could require a mailer to stop all future mailings if he or she received advertisements that he or she believed to be erotically arousing or sexually provocative. Although it was the government that empowered individuals to avoid materials they considered provocative, the Court emphasized that the mailer's right to communicate was circumscribed only by an affirmative act of a householder. . . .

Like the do-not-mail regulation approved in *Rowan,* the national do-not-call registry does not itself prohibit any speech. Instead, it merely "permits a citizen to erect a wall . . . that no advertiser may penetrate without his acquiescence." *See Rowan,* 397 U.S. at 738. Almost by definition, the do-not-call regulations only block calls that would constitute unwanted intrusions into the privacy of consumers who have signed up for the list. . . .

NOTES & QUESTIONS

1. ***The Do Not Call List and* Rowan.** To what extent is this case controlled by *Rowan*? Does the Do Not Call (DNC) list go beyond the statute in *Rowan*?
2. ***Charitable and Political Calls.*** The DNC list permits calls based on charitable or political purposes. There is no way to block such calls. Suppose that Congress decided that all calls could be included. Would a charity or political group have a First Amendment ground to overturn the DNC list?

U.S. WEST, INC. V. FEDERAL COMMUNICATIONS COMMISSION

182 F.3d 1224 (10th Cir. 1999)

TACHA, J. . . . U.S. West, Inc. petitions for review of a Federal Communication Commission ("FCC") order restricting the use and disclosure of and access to customer proprietary network information ("CPNI"). *See* 63 Fed. Reg. 20,326 (1998) ("CPNI Order"). [U.S. West argues that FCC regulations, implementing 47 U.S.C. § 222, among other things, violate the First Amendment. These regulations require telecommunications companies to ask consumers for approval (to "opt-in") before they can use a customer's personal information for marketing purposes.] . . .

The dispute in this case involves regulations the FCC promulgated to implement provisions of 47 U.S.C. § 222, which was enacted as part of the Telecommunications Act of 1996. Section 222, entitled "Privacy of customer information," states generally that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers." To effectuate that duty, § 222 places restrictions on the use, disclosure

a material degree.". . . On the record before us, the government fails to meet its burden.

The government presents no evidence showing the harm to either privacy or competition is real. Instead, the government relies on speculation that harm to privacy and competition for new services will result if carriers use CPNI. . . . While protecting against disclosure of sensitive and potentially embarrassing personal information may be important in the abstract, we have no indication of how it may occur in reality with respect to CPNI. Indeed, we do not even have indication that the disclosure might actually occur. The government presents no evidence regarding how and to whom carriers would disclose CPNI. . . . [T]he government has not explained how or why a carrier would disclose CPNI to outside parties, especially when the government claims CPNI is information that would give one firm a competitive advantage over another. This leaves us unsure exactly who would potentially receive the sensitive information. . . .

In order for a regulation to satisfy this final *Central Hudson* prong, there must be a fit between the legislature's means and its desired objective. . . .

. . . [O]n this record, the FCC's failure to adequately consider an obvious and substantially less restrictive alternative, an opt-out strategy, indicates that it did not narrowly tailor the CPNI regulations regarding customer approval. . . .

The respondents merely speculate that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so. Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires. . . .

In sum, even assuming that respondents met the prior two prongs of *Central Hudson,* we conclude that based on the record before us, the agency has failed to satisfy its burden of showing that the customer approval regulations restrict no more speech than necessary to serve the asserted state interests. Consequently, we find that the CPNI regulations interpreting the customer approval requirement of 47 U.S.C. § 222(c) violate the First Amendment.

BRISCOE, J. dissenting. . . . After reviewing the CPNI Order and the administrative record, I am convinced the FCC's interpretation of § 222, more specifically its selection of the opt-in method for obtaining customer approval, is entirely reasonable. Indeed, the CPNI Order makes a strong case that, of the two options seriously considered by the FCC, the opt-in method is the only one that legitimately forwards Congress' goal of ensuring that customers give informed consent for use of their individually identifiable CPNI. . . .

. . . U.S. West suggests the CPNI Order unduly limits its ability to engage in commercial speech with its existing customers regarding new products and services it may offer. . . .

The problem with U.S. West's arguments is they are more appropriately aimed at the restrictions and requirements outlined in § 222 rather than the approval method adopted in the CPNI Order. As outlined above, it is the statute, not the CPNI Order, that prohibits a carrier from using, disclosing, or permitting access to individually identifiable CPNI without first obtaining informed consent from its customers. Yet U.S. West has not challenged the constitutionality of § 222, and

this is not the proper forum for addressing such a challenge even if it was raised. . . .

The majority, focusing at this point on the CPNI Order rather than the statute, concludes the FCC failed to adequately consider the opt-out method, which the majority characterizes as "an obvious and substantially less restrictive alternative" than the opt-in method. Notably, however, the majority fails to explain why, in its view, the opt-out method is substantially less restrictive. Presumably, the majority is relying on the fact that the opt-out method typically results in a higher "approval" rate than the opt-in method. Were mere "approval" percentages the only factor relevant to our discussion, the majority would perhaps be correct. As the FCC persuasively concluded in the CPNI Order, however, the opt-out method simply does not comply with § 222's requirement of informed consent. In particular, the opt-out method, unlike the opt-in method, does not guarantee that a customer will make an informed decision about usage of his or her individually identifiable CPNI. To the contrary, the opt-out method creates the very real possibility of "uninformed" customer approval. In the end, I reiterate my point that the opt-in method selected by the FCC is the only method of obtaining approval that serves the governmental interests at issue while simultaneously complying with the express requirement of the statute (i.e., obtaining informed customer consent). . . .

In conclusion, I view U.S. West's petition for review as little more than a run-of-the-mill attack on an agency order "clothed by ingenious argument in the garb" of First Amendment issues. . . .

NOTES & QUESTIONS

1. ***The Aftermath of* U.S. West: *The FCC and the D.C. Circuit.*** The FCC responded to the *U.S. West* decision at length in its 2007 CPNI Order and largely rejected its holdings. FCC Report and Order, 07-22 (April 2, 2007). The one change that it made was to modify its 1998 Order at issue in *U.S. West* so that opt-in consent would be required only with respect to a carrier's sharing of customer information with third-party marketers.

   The FCC also declared that the Tenth Circuit in *U.S. West* had based its decision "on a different record than the one compiled here" and in particular on premises that were no longer valid. First, the FCC reasoned, there was now ample evidence of disclosure of CPNI and the adverse effects it could have on customers. Second, there was now substantial evidence that an opt-out strategy would not adequately protect customer privacy "because most customers either do not read or do not understand carriers' opt-out notices." The FCC also stated that requiring opt-in consent from customers before sharing CPNI with joint venture partners and independent contractors for marketing purposes would pass First Amendment scrutiny.

   The D.C. Circuit upheld the FCC's 2007 Report and Order. *National Cable and Telecommunications Association*, 555 F.3d 996 (D.C. Cir. 2009). It found that the government had a "substantial" interest, under the *Central Hudson* test, in "protecting the privacy of consumer credit information." In its analysis of the second part of the *Central Hudson* test, the D.C. Circuit found that the Commission's 2007 Order "directly advances" the government's interest:

> [C]ommon sense supports the Commission's determination that the risk of unauthorized disclosure of customer information increases with the number of entities possessing it. The Commission therefore reasonably concluded that an opt-in consent requirement directly and materially advanced the interests in protecting customer privacy and in ensuring customer control over the information.

Finally, the court found that under *Central Hudson*'s final requirement the 2007 Report and Order easily met the standard of a regulation proportionate to the government's interest. The court reasoned that the difference between opt in and opt out is only a marginal one in the relative degree of burden on First Amendment interests. The D.C. Circuit found that the "Commission carefully considered the differences between the two regulatory approaches, and the evidence supports the Commission's decision to prefer opt-in consent."

If the *U.S. West* court were to examine the FCC's 2007 Report and Order, would it likely agree or disagree with the D.C. Circuit?

2. ***Is Opt In Narrowly Tailored?*** Is the opt-in system involved in *U.S. West* more restrictive than the do-not-mail list in *Rowan* or the DNC list in *Mainstream Marketing*? Is the privacy interest in *U.S. West* different than in *Rowan* and *Mainstream Marketing*?
3. ***Personal Information: Property, Contract, and Speech.*** Consider the following critique of *U.S. West* by Julie Cohen:

> The law affords numerous instances of regulation of the exchange of information as property or product. Securities markets, which operate entirely by means of information exchange, are subject to extensive regulation, and hardly anybody thinks that securities laws and regulations should be subjected to heightened or strict First Amendment scrutiny. Laws prohibiting patent, copyright, and trademark infringement, and forbidding the misappropriation of trade secrets, have as their fundamental purpose (and their undisputed effect) the restriction of information flows. The securities and intellectual property laws, moreover, are expressly content-based, and thus illustrate that (as several leading First Amendment scholars acknowledge) this characterization doesn't always matter. Finally, federal computer crime laws punish certain uses of information for reasons entirely unrelated to their communicative aspects. . . .
>
> The accumulation, use, and market exchange of personally-identified data don't fit neatly into any recognized category of "commercial speech" . . . because in the ways that matter, these activities aren't really "speech" at all. Although regulation directed at these acts may impose some indirect burden on direct-to-consumer communication, that isn't the primary objective of data privacy regulation. This suggests that, at most, data privacy regulation should be subject to the intermediate scrutiny applied to indirect speech regulation.[96]

4. ***Is Opt In Too Expensive?*** Michael Staten and Fred Cate have defended the *U.S. West* decision by noting the results of the testing of an opt-in system by U.S. West:

[96] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1416-18, 1421 (2000).

> In 1997, U.S. West (now Qwest Communications), one of the largest telecommunications companies in the United States, conducted one of the few affirmative consent trials for which results are publicly available. In that trial, the company sought permission from its customers to utilize information about their calling patterns (e.g., volume of calls, time and duration of calls, etc.) to market new services to them. The direct mail appeal for permission received a positive response rate between 5 and 11 percent for residential customers (depending upon the size of a companion incentive offered by the company). Residential customers opted in at a rate of 28 percent when called about the service.
>
> When U.S. West was actually communicating in person with the consumers, the positive response rate was three to six times higher than when it relied on consumers reading and responding to mail. But even with telemarketing, the task of reaching a customer is daunting. U.S. West determined that it required an average of 4.8 calls to each consumer household before they reached an adult who could grant consent. In one-third of households called, U.S. West never reached the customer, despite repeated attempts. In any case, many U.S. West customers received more calls than would have been the case in an opt-out system, and despite repeated contact attempts, one-third of their customers missed opportunities to receive new products and services. The approximately $20 cost per positive response in the telemarketing test and $29 to $34 cost per positive response in the direct mail test led the company to conclude that opt-in was not a viable business model because it was too costly, too difficult, and too time intensive.[97]

Robert Gellman, however, generally disputes the findings of industry studies about the costs of privacy protective measures. With regard to opt-in cost assessments, Gellman argues that industry studies often fail "to consider other ways [beyond direct mail and telemarketing] that business and charities can solicit individuals to replace any losses from opt-in requirements. Newspaper, Internet, radio, and television advertising may be effective substitutes for direct mail. There are other ways to approach individuals without the compilation of detailed personal dossiers. None of the alternatives is adequately considered."[98]

5. ***Is Commercial Transaction Information Different from Other Speech?*** Courts analyzing First Amendment challenges to regulation of data about commercial transactions have typically viewed the dissemination and use of such data as commercial speech, and they have applied the *Central Hudson* test. This test is less protective than regular First Amendment protection. Solveig Singleton contends that data about commercial transactions should be considered regular speech, not commercial speech:

> Is commercial tracking essentially different from gossip? . . .
>
> Gossip and other informal personal contacts serve an important function in advanced economies. In Nineteenth Century America, entrepreneurs would increase their sales by acquiring information about their customers. Customers

[97] Michael E. Staten & Fred H. Cate, *The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA*, 52 Duke L.J. 745, 767-68 (2003).

[98] Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs Are Biased and Incomplete* (Mar. 2002), at http://www.epic.org/reports/dmfprivacy.html.

> relied on their neighborhood banker, whom they knew since childhood, to grant them credit. They would return again and again to the same stores for personalized service. . . .
>
> [E]conomic actors must develop new mechanisms of relaying information to each other about fraud, trust, and behavior of potential customers. Towards the end of the Nineteenth Century and throughout the Twentieth Century, formal credit reporting began to evolve out of gossip networks. . . .
>
> The equivalence of gossip and consumer databases suggests that there is no need to treat the evolution of databases as a crisis. Those who argue for a new legal regime for privacy, however, view new uses of information as having crossed an "invisible line" between permissible gossip and violative information collection. While the use of new technology to collect information may make people uneasy, is there any reason to suppose that any harm that might result will amount to greater harm than the harm that could come from being a victim of vicious gossip?[99]

Singleton goes on to contend that information collected by businesses in databases is less pernicious than gossip because few people have access to it and it is "likely to be much more accurate than gossip." Is the information in computer databases merely gossip on a more systemic scale? Compare how the First Amendment regulates gossip with how it regulates commercial speech.

6. ***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 fixes the 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.[100]

[99] Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 Fordham Intell. Prop. Media & Ent. L.J. 97, 126-32 (2000).

[100] James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. Colo. L. Rev. 1, 29-36, 42 (2005).

TRANS UNION CORP. v. FEDERAL TRADE COMMISSION

245 F.3d 809 (D.C. Cir. 2001)

TATEL, J. . . . Petitioner Trans Union sells two types of products. First, as a credit reporting agency, it compiles credit reports about individual consumers from credit information it collects from banks, credit card companies, and other lenders. It then sells these credit reports to lenders, employers, and insurance companies. Trans Union receives credit information from lenders in the form of "tradelines." A tradeline typically includes a customer's name, address, date of birth, telephone number, Social Security number, account type, opening date of account, credit limit, account status, and payment history. Trans Union receives 1.4 to 1.6 billion records per month. The company's credit database contains information on 190 million adults.

Trans Union's second set of products — those at issue in this case — are known as target marketing products. These consist of lists of names and addresses of individuals who meet specific criteria such as possession of an auto loan, a department store credit card, or two or more mortgages. Marketers purchase these lists, then contact the individuals by mail or telephone to offer them goods and services. To create its target marketing lists, Trans Union maintains a database known as MasterFile, a subset of its consumer credit database. MasterFile consists of information about every consumer in the company's credit database who has (A) at least two tradelines with activity during the previous six months, or (B) one tradeline with activity during the previous six months plus an address confirmed by an outside source. The company compiles target marketing lists by extracting from MasterFile the names and addresses of individuals with characteristics chosen by list purchasers. For example, a department store might buy a list of all individuals in a particular area code who have both a mortgage and a credit card with a $10,000 limit. Although target marketing lists contain only

names and addresses, purchasers know that every person on a list has the characteristics they requested because Trans Union uses those characteristics as criteria for culling individual files from its database. Purchasers also know that every individual on a target marketing list satisfies the criteria for inclusion in MasterFile.

The Fair Credit Reporting Act of 1970 ("FCRA"), 15 U.S.C. §§ 1681, 1681a-1681u, regulates consumer reporting agencies like Trans Union, imposing various obligations to protect the privacy and accuracy of credit information. The Federal Trade Commission, acting pursuant to its authority to enforce the FCRA, *see* 15 U.S.C. § 1681s(a), determined that Trans Union's target marketing lists were "consumer reports" subject to the Act's limitations. [The FTC concluded that targeted marketing was not an authorized use of consumer reports under the FCRA and ordered Trans Union to halt its sale of the lists.] . . .

. . . [Trans Union challenges the FTC's application of the FCRA as violative of the First Amendment.] Banning the sale of target marketing lists, the company says, amounts to a restriction on its speech subject to strict scrutiny. Again, Trans Union misunderstands our standard of review. In *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749 (1985), the Supreme Court held that a consumer reporting agency's credit report warranted reduced constitutional protection because it concerned "no public issue." "The protection to be accorded a particular credit report," the Court explained, "depends on whether the report's 'content, form, and context' indicate that it concerns a public matter." Like the credit report in *Dun & Bradstreet,* which the Supreme Court found "was speech solely in the interest of the speaker and its specific business audience," the information about individual consumers and their credit performance communicated by Trans Union target marketing lists is solely of interest to the company and its business customers and relates to no matter of public concern. Trans Union target marketing lists thus warrant "reduced constitutional protection."

We turn then to the specifics of Trans Union's First Amendment argument. The company first claims that neither the FCRA nor the Commission's Order advances a substantial government interest. The "Congressional findings and statement of purpose" at the beginning of the FCRA state: "There is a need to insure that consumer reporting agencies exercise their grave responsibilities with . . . respect for the consumer's right to privacy." 15 U.S.C. § 1681(a)(4). Contrary to the company's assertions, we have no doubt that this interest — protecting the privacy of consumer credit information — is substantial.

Trans Union next argues that Congress should have chosen a "less burdensome alternative," i.e., allowing consumer reporting agencies to sell credit information as long as they notify consumers and give them the ability to "opt out." Because the FCRA is not subject to strict First Amendment scrutiny, however, Congress had no obligation to choose the least restrictive means of accomplishing its goal.

Finally, Trans Union argues that the FCRA is underinclusive because it applies only to consumer reporting agencies and not to other companies that sell consumer information. But given consumer reporting agencies' unique "access to a broad range of continually-updated, detailed information about millions of consumers' personal credit histories," we think it not at all inappropriate for Congress to have singled out consumer reporting agencies for regulation. . . .

NOTES & QUESTIONS

1. **U.S. West *vs.* Trans Union.** Compare *U.S. West* with *Trans Union*. Are these cases consistent with each other? Which case's reasoning strikes you as more persuasive?
2. **Trans Union II.** In *Trans Union v. FTC*, 295 F.3d 42 (D.C. Cir. 2002) (*Trans Union II*), Trans Union sued to enjoin regulations promulgated pursuant to the Gramm-Leach-Bliley Act (GLBA), alleging, among other things, that they violated the First Amendment. Trans Union argued that these regulations would prevent it from selling credit headers, which consist of a consumer's name, address, Social Security number, and phone number. Trans Union contended that the sale of credit headers is commercial speech. The court concluded that Trans Union's First Amendment arguments were "foreclosed" by its earlier opinion in *Trans Union v. FTC,* which resolved that "the government interest in 'protecting the privacy of consumer credit information' 'is substantial.'"
3. ***Free Speech and the Fair Information Practices.*** Recall the discussion of the Fair Information Practices from Chapter 6. The Fair Information Practices provide certain limitations on the uses and disclosure of personal information. Eugene Volokh contends:

> I am especially worried about the normative power of the notion that the government has a compelling interest in creating "codes of fair information practices" restricting true statements made by nongovernmental speakers. The protection of free speech generally rests on an assumption that it's not for the government to decide which speech is "fair" and which isn't; the unfairnesses, excesses, and bad taste of speakers are something that current First Amendment principles generally require us to tolerate. Once people grow to accept and even like government restrictions on one kind of supposedly "unfair" communication of facts, it may become much easier for people to accept "codes of fair reporting," "codes of fair debate," "codes of fair filmmaking," "codes of fair political criticism," and the like. . . .[101]

Consider Paul Schwartz, who contends that free discourse is promoted by the protection of privacy:

> When the government requires fair information practices for the private sector, has it created a right to stop people from speaking about you? As an initial point, I emphasize that the majority of the core fair information practices do not involve the government preventing disclosure of personal information. [The fair information practices generally require: (1) the creation of a statutory fabric that defines obligations with respect to the use of personal information; (2) the maintenance of processing systems that are understandable to the concerned individual (transparency); (3) the assignment of limited procedural and substantive rights to the individual; and (4) the establishment of effective oversight of data use, whether through individual litigation (self-help), a government role (external oversight), or some combination of these approaches.] . . . [F]air information practices one, two, and four regulate the business practices of private entities without silencing their speech. No

[101] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049, 1090 (2000).

prevention of speech about anyone takes place, for example, when the Fair Credit Reporting Act of 1970 requires that certain information be given to a consumer when an "investigative consumer report" is prepared about her.

These nonsilencing fair information practices are akin to a broad range of other measures that regulate information use in the private sector and do not abridge the freedom of speech under any interpretation of the First Amendment. The First Amendment does not prevent the government from requiring product labels on food products or the use of "plain English" by publicly traded companies in reports sent to their investors or Form 10-Ks filed with the Securities and Exchange Commission. Nor does the First Amendment forbid privacy laws such as the Children's Online Privacy Protection Act, which assigns parents a right of access to their children's online data profiles. The ultimate merit of these laws depends on their specific context and precise details, but such experimentation by the State should be viewed as noncontroversial on free speech grounds.

Nevertheless, one subset of fair information practices does correspond to Volokh's idea of information privacy as the right to stop people from speaking about you. . . . [S]o long as [laws protecting personal information disclosure] are viewpoint neutral, these laws are a necessary element of safeguarding free communication in our democratic society. . . .

. . . [A] democratic order depends on both an underlying personal capacity for self-governance and the participation of individuals in community and democratic self-rule. Privacy law thus has an important role in protecting individual self-determination and democratic deliberation. By providing access to one's personal data, information about how it will be processed, and other fair information practices, the law seeks to structure the terms on which individuals confront the information demands of the community, private bureaucratic entities, and the State. Attention to these issues by the legal order is essential to the health of a democracy, which ultimately depends on individual communicative competence.[102]

SORRELL v. IMS HEALTH, INC.

131 S. Ct. 2653 (2011)

KENNEDY, J. Vermont law restricts the sale, disclosure, and use of pharmacy records that reveal the prescribing practices of individual doctors. Vt. Stat. Ann., Tit. 18, § 4631. Subject to certain exceptions, the information may not be sold, disclosed by pharmacies for marketing purposes, or used for marketing by pharmaceutical manufacturers. Vermont argues that its prohibitions safeguard medical privacy and diminish the likelihood that marketing will lead to prescription decisions not in the best interests of patients or the State. It can be assumed that these interests are significant. Speech in aid of pharmaceutical marketing, however, is a form of expression protected by the Free Speech Clause of the First Amendment. As a consequence, Vermont's statute must be subjected to heightened judicial scrutiny. The law cannot satisfy that standard. . . .

Pharmaceutical manufacturers promote their drugs to doctors through a process called "detailing." This often involves a scheduled visit to a doctor's office

[102] Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence,* 52 Stan. L. Rev. 1559 (2000).

to persuade the doctor to prescribe a particular pharmaceutical. Detailers bring drug samples as well as medical studies that explain the "details" and potential advantages of various prescription drugs. Interested physicians listen, ask questions, and receive followup data. Salespersons can be more effective when they know the background and purchasing preferences of their clientele, and pharmaceutical salespersons are no exception. Knowledge of a physician's prescription practices—called "prescriber-identifying information"—enables a detailer better to ascertain which doctors are likely to be interested in a particular drug and how best to present a particular sales message. Detailing is an expensive undertaking, so pharmaceutical companies most often use it to promote high-profit brand-name drugs protected by patent. Once a brand-name drug's patent expires, less expensive bioequivalent generic alternatives are manufactured and sold.

Pharmacies, as a matter of business routine and federal law, receive prescriber-identifying information when processing prescriptions. Many pharmacies sell this information to "data miners," firms that analyze prescriber-identifying information and produce reports on prescriber behavior. Data miners lease these reports to pharmaceutical manufacturers subject to nondisclosure agreements. Detailers, who represent the manufacturers, then use the reports to refine their marketing tactics and increase sales.

In 2007, Vermont enacted the Prescription Confidentiality Law. The measure is also referred to as Act 80. It has several components. The central provision of the present case is § 4631(d).

> "A health insurer, a self-insured employer, an electronic transmission intermediary, a pharmacy, or other similar entity shall not sell, license, or exchange for value regulated records containing prescriber-identifiable information, nor permit the use of regulated records containing prescriber-identifiable information for marketing or promoting a prescription drug, unless the prescriber consents . . . . Pharmaceutical manufacturers and pharmaceutical marketers shall not use prescriber-identifiable information for marketing or promoting a prescription drug unless the prescriber consents. . . ."

The quoted provision has three component parts. The provision begins by prohibiting pharmacies, health insurers, and similar entities from selling prescriber-identifying information, absent the prescriber's consent. . . . The provision then goes on to prohibit pharmacies, health insurers, and similar entities from allowing prescriber-identifying information to be used for marketing, unless the prescriber consents. This prohibition in effect bars pharmacies from disclosing the information for marketing purposes. Finally, the provision's second sentence bars pharmaceutical manufacturers and pharmaceutical marketers from using prescriber-identifying information for marketing, again absent the prescriber's consent. The Vermont attorney general may pursue civil remedies against violators. § 4631(f). . . .

On its face, Vermont's law enacts content- and speaker-based restrictions on the sale, disclosure, and use of prescriber-identifying information. The provision first forbids sale subject to exceptions based in large part on the content of a purchaser's speech. For example, those who wish to engage in certain "educational communications," § 4631(e)(4), may purchase the information. The measure then bars any disclosure when recipient speakers will use the information for marketing.

Finally, the provision's second sentence prohibits pharmaceutical manufacturers from using the information for marketing. The statute thus disfavors marketing, that is, speech with a particular content. More than that, the statute disfavors specific speakers, namely pharmaceutical manufacturers. As a result of these content- and speaker-based rules, detailers cannot obtain prescriber-identifying information, even though the information may be purchased or acquired by other speakers with diverse purposes and viewpoints. . . . For example, it appears that Vermont could supply academic organizations with prescriber-identifying information to use in countering the messages of brand-name pharmaceutical manufacturers and in promoting the prescription of generic drugs. But § 4631(d) leaves detailers no means of purchasing, acquiring, or using prescriber-identifying information. The law on its face burdens disfavored speech by disfavored speakers. . . .

Act 80 is designed to impose a specific, content-based burden on protected expression. It follows that heightened judicial scrutiny is warranted. . . . Vermont's law does not simply have an effect on speech, but is directed at certain content and is aimed at particular speakers. The Constitution "does not enact Mr. Herbert Spencer's Social Statics." *Lochner v. New York*, 198 U.S. 45 (1905) (Holmes, J., dissenting). It does enact the First Amendment.

This Court has held that the creation and dissemination of information are speech within the meaning of the First Amendment. *See, e.g., Bartnicki* ("[I]f the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct"). Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes.

The State asks for an exception to the rule that information is speech, but there is no need to consider that request in this case. The State has imposed content- and speaker-based restrictions on the availability and use of prescriber-identifying information. So long as they do not engage in marketing, many speakers can obtain and use the information. But detailers cannot. Vermont's statute could be compared with a law prohibiting trade magazines from purchasing or using ink. As a consequence, this case can be resolved even assuming, as the State argues, that prescriber-identifying information is a mere commodity. . . .

The State's asserted justifications for § 4631(d) come under two general headings. First, the State contends that its law is necessary to protect medical privacy, including physician confidentiality, avoidance of harassment, and the integrity of the doctor-patient relationship. Second, the State argues that § 4631(d) is integral to the achievement of policy objectives—namely, improved public health and reduced healthcare costs. Neither justification withstands scrutiny.

Vermont argues that its physicians have a "reasonable expectation" that their prescriber-identifying information "will not be used for purposes other than . . . filling and processing" prescriptions. It may be assumed that, for many reasons, physicians have an interest in keeping their prescription decisions confidential. But § 4631(d) is not drawn to serve that interest. Under Vermont's law, pharmacies may share prescriber-identifying information with anyone for any reason save one: They must not allow the information to be used for marketing. . . .

Perhaps the State could have addressed physician confidentiality through "a more coherent policy." *Greater New Orleans Broadcasting*, [527 U.S. 173, 195 (1999)]. For instance, the State might have advanced its asserted privacy interest by allowing the information's sale or disclosure in only a few narrow and well-justified circumstances. *See, e.g.,* Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d–2; 45 CFR pts. 160 and 164. A statute of that type would present quite a different case than the one presented here. But the State did not enact a statute with that purpose or design. Instead, Vermont made prescriber-identifying information available to an almost limitless audience. The explicit structure of the statute allows the information to be studied and used by all but a narrow class of disfavored speakers. Given the information's widespread availability and many permissible uses, the State's asserted interest in physician confidentiality does not justify the burden that § 4631(d) places on protected expression.

. . . Section 4631(d) may offer a limited degree of privacy, but only on terms favorable to the speech the State prefers. Cf. *Rowan* (sustaining a law that allowed private parties to make "unfettered," "unlimited," and "unreviewable" choices regarding their own privacy). This is not to say that all privacy measures must avoid content-based rules. Here, however, the State has conditioned privacy on acceptance of a content-based rule that is not drawn to serve the State's asserted interest. To obtain the limited privacy allowed by § 4631(d), Vermont physicians are forced to acquiesce in the State's goal of burdening disfavored speech by disfavored speakers.

The State also contends that § 4631(d) protects doctors from "harassing sales behaviors." It is doubtful that concern for "a few" physicians who may have "felt coerced and harassed" by pharmaceutical marketers can sustain a broad content-based rule like § 4631(d). Many are those who must endure speech they do not like, but that is a necessary cost of freedom. In any event the State offers no explanation why remedies other than content-based rules would be inadequate. Physicians can, and often do, simply decline to meet with detailers, including detailers who use prescriber-identifying information. Doctors who wish to forgo detailing altogether are free to give "No Solicitation" or "No Detailing" instructions to their office managers or to receptionists at their places of work. . . .

Vermont argues that detailers' use of prescriber-identifying information undermines the doctor-patient relationship by allowing detailers to influence treatment decisions. . . . But the State does not explain why detailers' use of prescriber-identifying information is more likely to prompt these objections than many other uses permitted by § 4631(d). In any event, this asserted interest is contrary to basic First Amendment principles. . . . If pharmaceutical marketing affects treatment decisions, it does so because doctors find it persuasive. Absent circumstances far from those presented here, the fear that speech might persuade provides no lawful basis for quieting it.

The State contends that § 4631(d) advances important public policy goals by lowering the costs of medical services and promoting public health. If prescriber-identifying information were available for use by detailers, the State contends, then detailing would be effective in promoting brand-name drugs that are more expensive and less safe than generic alternatives. . . . While Vermont's stated policy goals may be proper, § 4631(d) does not advance them in a permissible

way. . . . The State seeks to achieve its policy objectives through the indirect means of restraining certain speech by certain speakers—that is, by diminishing detailers' ability to influence prescription decisions. Those who seek to censor or burden free expression often assert that disfavored speech has adverse effects. But the "fear that people would make bad decisions if given truthful information" cannot justify content-based burdens on speech. . . .

It is true that content-based restrictions on protected expression are sometimes permissible, and that principle applies to commercial speech. . . . Here, however, Vermont has not shown that its law has a neutral justification.

The State nowhere contends that detailing is false or misleading within the meaning of this Court's First Amendment precedents. Nor does the State argue that the provision challenged here will prevent false or misleading speech. The State's interest in burdening the speech of detailers instead turns on nothing more than a difference of opinion. . . .

The capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure. In considering how to protect those interests, however, the State cannot engage in content-based discrimination to advance its own side of a debate.

If Vermont's statute provided that prescriber-identifying information could not be sold or disclosed except in narrow circumstances then the State might have a stronger position. Here, however, the State gives possessors of the information broad discretion and wide latitude in disclosing the information, while at the same time restricting the information's use by some speakers and for some purposes, even while the State itself can use the information to counter the speech it seeks to suppress. Privacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the government prefers. . . .

The State has burdened a form of protected expression that it found too persuasive. At the same time, the State has left unburdened those speakers whose messages are in accord with its own views. This the State cannot do. . . .

BREYER, J., joined by GINSBURG, J. and KAGAN, J., dissenting. The Vermont statute before us adversely affects expression in one, and only one, way. It deprives pharmaceutical and data-mining companies of data, collected pursuant to the government's regulatory mandate, that could help pharmaceutical companies create better sales messages. In my view, this effect on expression is inextricably related to a lawful governmental effort to regulate a commercial enterprise. The First Amendment does not require courts to apply a special "heightened" standard of review when reviewing such an effort. And, in any event, the statute meets the First Amendment standard this Court has previously applied when the government seeks to regulate commercial speech. For any or all of these reasons, the Court should uphold the statute as constitutional. . . .

In this case I would ask whether Vermont's regulatory provisions work harm to First Amendment interests that is disproportionate to their furtherance of legitimate regulatory objectives. . . .

[O]ur cases make clear that the First Amendment offers considerably less protection to the maintenance of a free marketplace for goods and services. And they also reflect the democratic importance of permitting an elected government to implement through effective programs policy choices for which the people's elected representatives have voted. . . .

Vermont's statute neither forbids nor requires anyone to say anything, to engage in any form of symbolic speech, or to endorse any particular point of view, whether ideological or related to the sale of a product. . . . Further, the statute's requirements form part of a traditional, comprehensive regulatory regime. The pharmaceutical drug industry has been heavily regulated at least since 1906. Longstanding statutes and regulations require pharmaceutical companies to engage in complex drug testing to ensure that their drugs are both "safe" and "effective." 21 U.S.C. §§ 355(b)(1), 355(d). Only then can the drugs be marketed, at which point drug companies are subject to the FDA's exhaustive regulation of the content of drug labels and the manner in which drugs can be advertised and sold.

Finally, Vermont's statute is directed toward information that exists only by virtue of government regulation. Under federal law, certain drugs can be dispensed only by a pharmacist operating under the orders of a medical practitioner. 21 U.S.C. § 355(b). Vermont regulates the qualifications, the fitness, and the practices of pharmacists themselves, and requires pharmacies to maintain a "patient record system" that, among other things, tracks who prescribed which drugs. But for these regulations, pharmacies would have no way to know who had told customers to buy which drugs (as is the case when a doctor tells a patient to take a daily dose of aspirin).

Regulators will often find it necessary to create tailored restrictions on the use of information subject to their regulatory jurisdiction. A car dealership that obtains credit scores for customers who want car loans can be prohibited from using credit data to search for new customers. *See* 15 U.S.C. § 1681b; *cf. Trans Union Corp. v. FTC*, 245 F.3d 809, *reh'g denied*, 267 F.3d 1138 (D.C. Cir. 2001). Medical specialists who obtain medical records for their existing patients cannot purchase those records in order to identify new patients. *See* 45 CFR § 164.508(a)(3). Or, speaking hypothetically, a public utilities commission that directs local gas distributors to gather usage information for individual customers might permit the distributors to share the data with researchers (trying to lower energy costs) but forbid sales of the data to appliance manufacturers seeking to sell gas stoves. . . . Thus, it is not surprising that, until today, this Court has *never* found that the First Amendment prohibits the government from restricting the use of information gathered pursuant to a regulatory mandate—whether the information rests in government files or has remained in the hands of the private firms that gathered it.

In short, the case law in this area reflects the need to ensure that the First Amendment protects the "marketplace of ideas," thereby facilitating the democratic creation of sound government policies without improperly hampering the ability of government to introduce an agenda, to implement its policies, and to favor them to the exclusion of contrary policies. To apply "heightened" scrutiny when the regulation of commercial activities (which often involve speech) is at issue is unnecessarily to undercut the latter constitutional goal. The majority's view of this case presents that risk. . . .

Moreover, given the sheer quantity of regulatory initiatives that touch upon commercial messages, the Court's vision of its reviewing task threatens to return us to a happily bygone era when judges scrutinized legislation for its interference with economic liberty. History shows that the power was much abused and resulted in the constitutionalization of economic theories preferred by individual jurists. *See Lochner v. New York,* 198 U.S. 45 (1905) (Holmes, J., dissenting). . . .

The statute threatens only modest harm to commercial speech. I agree that it withholds from pharmaceutical companies information that would help those entities create a more effective selling message. But I cannot agree with the majority that the harm also involves unjustified discrimination in that it permits "pharmacies" to "share prescriber-identifying information with anyone for any reason" (but marketing). Whatever the First Amendment relevance of such discrimination, there is no evidence that it exists in Vermont. The record contains no evidence that prescriber-identifying data is widely disseminated. . . .

The legitimate state interests that the statute serves are "substantial." *Central Hudson*, 447 U.S., at 564. . . . The protection of public health falls within the traditional scope of a State's police powers. The fact that the Court normally exempts the regulation of "misleading" and "deceptive" information even from the rigors of its "intermediate" commercial speech scrutiny testifies to the importance of securing "unbiased information," as does the fact that the FDA sets forth as a federal regulatory goal the need to ensure a "fair balance" of information about marketed drugs. As major payers in the health care system, health care spending is also of crucial state interest. And this Court has affirmed the importance of maintaining "privacy" as an important public policy goal—even in respect to information already disclosed to the public for particular purposes (but not others). *See Department of Justice v. Reporters Comm. for Freedom of Press,* 489 U.S. 749 (1989); *see also* Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 520–522 (2006); *cf. NASA v. Nelson,* 131 S. Ct. 746 (2011) (discussing privacy interests in nondisclosure). . . .

The record also adequately supports the State's privacy objective. Regulatory rules in Vermont make clear that the confidentiality of an individual doctor's prescribing practices remains the norm. Exceptions to this norm are comparatively few.

. . . The prohibition against pharmaceutical firms using this prescriber-identifying information works no more than modest First Amendment harm; the prohibition is justified by the need to ensure unbiased sales presentations, prevent unnecessarily high drug costs, and protect the privacy of prescribing physicians. There is no obvious equally effective, more limited alternative. . . .

In sum, I believe that the statute before us satisfies the "intermediate" standards this Court has applied to restrictions on commercial speech. *A fortiori* it satisfies less demanding standards that are more appropriately applied in this kind of commercial regulatory case—a case where the government seeks typical regulatory ends (lower drug prices, more balanced sales messages) through the use of ordinary regulatory means (limiting the commercial use of data gathered pursuant to a regulatory mandate). The speech-related consequences here are indirect, incidental, and entirely commercial. . . .

Regardless, whether we apply an ordinary commercial speech standard or a less demanding standard, I believe Vermont's law is consistent with the First Amendment. And with respect, I dissent.

NOTES & QUESTIONS

1. ***The Impact of* Sorrell.** The Supreme Court takes an expansive view of commercial speech, which encompasses the sale and use of personal data. What kind of impact will this case likely have on other privacy laws regulating the trade of personal data? Does *Sorrell* affect *Mainstream Marketing Services, Inc. v. FTC* (excerpted above)? Does it affect the *Trans Union* cases (excerpted and discussed above)? What likely impact, if any, will it have?
2. ***Narrow vs. Broad Laws.*** Ironically, the Court's decision to strike down the law was based in part on how narrowly the law restricted the use or disclosure of personal data. How would you redraft the law to address the Court's concerns?
3. ***HIPAA.*** The *Sorrell* Court characterizes HIPAA as a law "allowing the information's sale or disclosure in only a few narrow and well-justified circumstances." Is this an accurate characterization of HIPAA? If HIPAA's restrictions pass muster, then can *Sorrell* be read as a narrow holding that applies only to laws that single out one particular use or one particular group of speakers?
4. ***Is Information Speech?*** Is the collection, use, and/or transfer of personal information a form of speech? Or is it merely trade in property?

   Eugene Volokh contends that such information processing constitutes speech:

   > Many . . . databases — for instance, credit history databases or criminal record databases — are used by people to help them decide whom it is safe to deal with and who is likely to cheat them. Other databases, which contain less incriminating information, such as a person's shopping patterns . . . [contain] data [that] is of direct daily life interest to its recipients, since it helps them find out with whom they should do business.[103]

   Further, Volokh contends: "[I]t is no less speech when a credit bureau sends credit information to a business. The owners and managers of a credit bureau are communicating information to decision-makers, such as loan officers, at the recipient business."[104]

   Daniel Solove recognizes that some forms of database information transfer and use can constitute speech:

   > There are no easy analytic distinctions as to what is or is not "speech." The "essence" of information is neither a good, nor is it speech, for information can be used in ways that make it akin to either one. It is the *use* of the information that determines what information is, not anything inherent in the information itself. If I sell you a book, I have engaged in a commercial transaction. I sold the book as a good. However, the book is also expressing something. Even

[103] Volokh, *Freedom of Speech, supra,* at 1093-94.
[104] *Id.* at 1083-84.

though books are sold as goods, the government cannot pass a law restricting the topics of what books can be sold. . . .

Volokh appears to view all information dissemination that is communicative as speech. Under Volokh's view, therefore, most forms of information dissemination would be entitled to equal First Amendment protection. . . .

However, Volokh's view would lead to severe conflicts with much modern regulation. Full First Amendment protection would apply to statements about a company's earnings and other information regulated by the SEC, insider trading, quid pro quo sexual harassment, fraudulent statements, perjury, bribery, blackmail, extortion, conspiracy, and so on. One could neatly exclude these examples from the category of speech, eliminating the necessity for First Amendment analysis. Although this seems the easiest approach, it is conceptually sloppy or even dishonest absent a meaningful way to argue that these examples do not involve communication. I contend that these examples of highly regulated forms of communication have not received the full rigor of standard First Amendment analysis because of policy considerations. Categorizing them as nonspeech conceals these policy considerations under the façade of an analytical distinction that thus far has not been persuasively articulated.

I am not eschewing all attempts at categorization between speech and nonspeech. To do so would make the First Amendment applicable to virtually anything that is expressive or communicative. Still, the distinction as currently constituted hides its ideological character. . . .

Dealing with privacy issues by categorizing personal information as nonspeech is undesirable because it cloaks the real normative reasons for why society wants to permit greater regulation of certain communicative activity. Rather than focusing on distinguishing between speech and nonspeech, the determination about what forms of information to regulate should center on policy considerations. These policy considerations should turn on the uses of the information rather than on notions about the inherent nature of the information.[105]

Solove goes on to argue that although transfers of personal information may be speech, they are of lower value than other forms of free speech, such as political speech. He contends that whereas speech of public concern is of high value, speech of private concern is given a lower constitutional value, and hence less stringent scrutiny, as is commercial speech and other lower-value categories of speech.

Neil Richards, however, contends that "most privacy regulation that interrupts information flows in the context of an express or implied commercial relationship is neither 'speech' within the current meaning of the First Amendment, nor should it be viewed as such." He criticizes Schwartz and Solove because "they grant too much ground to the First Amendment critique, and may ultimately prove to be underprotective of privacy interests, particularly in the database context." Richards finds Solove's contextual balancing approach too messy to "provide meaningfully increased protection for privacy in the courts." Richards argues instead for a categorical solution and contends

[105] Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure,* 53 Duke L.J. 967, 979-80 (2003).

that much regulation of speech in the commercial context should be seen as falling entirely outside the scope of the heightened First Amendment scrutiny:

> This might be the case because the speech is threatening, obscene, or libelous, and thus part of the "established" categories of "unprotected speech." But it might also be the case because the speech is an insider trading tip, . . . an offer to create a monopoly in restraint of trade, or a breach of the attorney-client privilege. In either case, the speech would be outside the scope of the First Amendment and could be regulated as long as a rational basis existed for so doing. . . .
>
> [I]nformation disclosure rules that are the product of generally applicable laws fall outside the scope of the First Amendment. Where information is received by an entity in violation of some other legal rule — whether breach of contract, trespass, theft, or fraud — the First Amendment creates no barrier to the government's ability to prevent and punish disclosure. This is the case even if the information is newsworthy or otherwise of public concern. . . .
>
> From a First Amendment perspective, no such equivalently important social function [as dissemination of information by the press] . . . is played by database companies engaged in the trade of personal data. Indeed, a general law regulating the commercial trade in personal data by database, profiling, and marketing companies is far removed from the core speech protected by the First Amendment, and is much more like the "speech" outside the boundaries of heightened review.

Richards goes on to equate the First Amendment critique of privacy regulation to *Lochnerism,* where the Supreme Court in *Lochner v. New York,* 198 U.S. 45 (1905), struck down a statute regulating the hours bakers could work per week based on "freedom of contract." *Lochner* was, and remains, highly criticized for being an impediment to New Deal legislation by an activist ideological Court. Richards notes:

> [T]here are some fairly strong parallels between the traditional conception of *Lochner* and the First Amendment critique of data privacy legislation. Both theories are judicial responses to calls for legal regulation of the economic and social dislocations caused by rapid technological change. *Lochnerism* addressed a major socio-technological problem of the industrial age — the power differential between individuals and businesses in industrial working conditions, while the First Amendment critique is addressed to a major socio-technological problem of our information age — the power differential between individuals and businesses over information in the electronic environment. Both theories place a libertarian gloss upon the Constitution, interpreting it to mandate either "freedom of contract" or "freedom of information." Both theories seek to place certain forms of economic regulation beyond the power of legislatures to enact. And both theories are eagerly supported by business interests keen to immunize themselves from regulation under the aegis of Constitutional doctrine. To the extent that the First Amendment critique is similar to the traditional view of *Lochner,* then, its elevation of an economic right to first-order constitutional magnitude seems similarly dubious.[106]

[106] Neil Richards, *Reconciling Data Privacy and the First Amendment,* 52 UCLA L. Rev. 1149, 1169, 1180, 1172-73, 1206, 1212-13 (2005).