Golden Gate University Law Review

Volume 45 | Issue 3 Article 4

September 2015

Do-It-Yourself Privacy: The Need for Comprehensive Federal Privacy Legislation With a Private Right of Action

Alec Wheatley
Golden Gate University School of Law

COMMENT

DO-IT-YOURSELF PRIVACY: THE NEED FOR COMPREHENSIVE FEDERAL PRIVACY LEGISLATION WITH A PRIVATE RIGHT OF ACTION

*ALEC WHEATLEY**

INTRODUCTION

On Black Friday 2013, at the height of the holiday shopping season, seventy million[1] Target customer records were hacked in one of the largest U.S. retail data breaches to date.[2] The hacked data included account numbers and payment card information as well as the personal data of customers.[3] The breach required banks to perform a massive reissuance of credit cards to customers, costing hundreds of millions of dollars,[4] and created the need for Target customers who had recently shopped at the retailer to sign up for credit monitoring services as protection against

* J.D. Candidate, May 2015, Golden Gate University School of Law; B.A. Philosophy, December 2007, University of California, Berkeley. I would like to thank Professor William Gallagher, Adjunct Professor Jessica Blazer, and Adjunct Professor Ed Baskauskas for providing thoughtful read-throughs and commentary prior to publication. Thanks and deepest appreciation to my family for their love and support throughout law school.

[1] Brian Krebs, *The Target Breach, by the Numbers*, KREBS ON SECURITY (May 6, 2014), http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.

[2] Michael Riley, Ben Elgin, Dune Lawrence & Carol Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG BUSINESSWEEK: TECHNOLOGY, Mar. 13, 2014, www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p1.

[3] Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. TIMES, Jan. 10, 2014, www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0 (reporting that customer names and phone numbers, as well as physical and email addresses, were taken).

[4] Jennifer Bjorhus, *Banks Have Replaced 15.3 Million Cards Since Target Breach*, STAR-TRIBUNE, Jan. 29, 2014 (7:25 PM), www.startribune.com/banks-have-replaced-15-3m-cards-since-target-breach/242505661/.

future unauthorized charges to their accounts. Both banks and consumers have brought lawsuits against Target on account of the breach.[5] The breach has raised concerns that Target did not take the steps necessary to adequately protect the personal information of its customers.[6]

The risk is now greater than ever that consumers will have their personal data misappropriated. The recent Target breach demonstrates how vulnerable consumers can become through the simple act of going to the store and using a credit card. Both brick-and-mortar (think WalMart) and Internet-only (think Amazon) national retailers process huge numbers of customer transactions every day. The fact that modern retailers operate on such a large scale necessitates the consolidation of customer data into large databases, where it is stored and mined using big data analytics.[7] Such consolidation poses severe risks to consumers in the event that those databases are breached. Target is not alone in being a target for data thieves. In the months following the Target breach, Neiman Marcus,[8] Michaels,[9] and Home Depot[10] all suffered high-profile breaches related to stolen customer credit card information.

Data security is only one slice of the privacy pie. Consumers have more to fear than just a breach of their financial information. They have to be wary of companies that change privacy policies without notice, publish their personal email contacts without consent, and sell their personal information to advertisers for a profit.[11] In fact, companies are continually finding new ways to leverage the customer data they control by analyzing customer buying trends to discover new insights, which they can sell for a profit. In addition, with the rise of the Internet of

[5] Ed Treleven, *Class Action Lawsuit Filed Here Against Target over Huge Data Breach*, WIS. ST. J., Feb. 15, 2014 (8:30 AM), http://host.madison.com/news/local/class-action-lawsuit-filed-here-against-target-over-huge-data/article_6731b897-afa9-59cb-8cfa-86a8022b3cb2.html.

[6] Riley et al., *supra* note 2 (noting that although Target had a security system in place, it did not follow up when security alarms were raised).

[7] *See generally* EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), *available at* www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf (reviewing the impact Big Data is having, and will continue to have, on many aspects of society).

[8] Ben Elgin, Dune Lawrence & Michael Riley, *Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data*, BLOOMBERG BUS., Feb. 21, 2014, www.bloomberg.com/bw/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data.

[9] Brian Krebs, *3 Million Customer Credit, Debit Cards Stolen in Michaels, Aaron Brothers Breaches*, KREBS ON SECURITY (Apr. 17, 2014), http://krebsonsecurity.com/2014/04/3-million-customer-credit-debit-cards-stolen-in-michaels-aaron-brothers-breaches/.

[10] Ben Elgin, Michael Riley & Dune Lawrence, *Home Depot Hacked After Months of Security Warnings*, BLOOMBERG BUS., Sept. 18, 2014, www.bloomberg.com/bw/articles/2014-09-18/home-depot-hacked-wide-open.

[11] *See infra* Part III (discussing FTC enforcement actions against companies for violations of consumer privacy).

Things,[12] the data available about consumer habits is set to increase dramatically. This in turn has encouraged the rise of Big Data, which values the collection and analysis of data above all else and drives companies to collect and store ever-greater amounts of consumer data.[13]

Consumer desire for more privacy online has pushed a market for new social media apps claiming heightened privacy protections. Michael Heyward, co-founder and CEO of a new application called "Whisper," claims that the app is the "the safest place on the internet."[14] Ironically, the app has been found to track the locations of users even when they have explicitly opted out by turning the app geolocation feature off.[15]

The risk of breach from hackers and the fact that even a company that claims to strongly value privacy is tracking its users both implicate consumer privacy rights and demonstrate that the need is greater than ever for a comprehensive federal privacy law that sets the standard for how consumer data is to be stored and used.[16]

This Comment is concerned with informational privacy, as opposed to decisional privacy.[17] Informational privacy concerns the collection and use of personally identifiable information (PII),[18] which includes the personal details that consumers give to companies either online or face-to-face as a normal part of doing business with them.[19] The information that companies glean from their customers' buying habits often results in the creation of highly detailed customer dossiers, reflecting a large number of consumers' attributes.[20]

---

[12] EXEC. OFFICE OF THE PRESIDENT, *supra* note 7, at 2.

[13] *See generally id.*

[14] Paul Lewis & Dominic Rushe, *Revealed: How Whisper App Tracks "Anonymous" Users*, GUARDIAN: TECH., Oct. 16, 2014 (11:35 EDT), www.theguardian.com/world/2014/oct/16/-sp-revealed-whisper-app-tracking-users.

[15] *Id.*

[16] This is not to say that companies can ever become breach-proof, but a privacy law that sets minimum requirements for handling customer information would be an important step toward making data more secure.

[17] Dorothy Glancy, *At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 357, 360 (2000) (distinguishing between "informational privacy," which concerns control and use of personal information, and "autonomy privacy," which concerns personal decisions and choices).

[18] Memorandum from Peter R. Orszag, Dir., Office of Mgmt. & Budget, to the Heads of Exec. Dep'ts and Agencies app. 8 (June 25, 2010), *available at* www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf (PII "refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual").

[19] In addition, through the use of loyalty cards and purchase tracking, companies are able to aggregate additional information about consumers to create detailed customer profiles.

[20] *Privacy and Consumer Profiling*, ELECTRONIC PRIVACY INFO. CENTER, https://epic.org/privacy/profiling (last visited Apr. 20, 2015) (customer profile information may include details such as marital status, age, sex, race, geography, health information, religion, and income).

Despite the fact that there is an enormous amount of consumer data being collected every day by companies, there is no comprehensive federal law establishing the proper standards for how that data is to be securely stored and transferred.[21] Once a consumer has consented to a company's collection of his or her personal information, with few exceptions the company is free to use it as it wishes.[22] When consumers share information with a company online, they should be able to feel confident that it will not be shared with third parties without their permission, and if it is stored, that it will be properly stored. Strict guidelines need to be laid down that describe the proper scope of use for consumer data based on the context in which that information is given.[23] This will prevent companies from exceeding the scope of consent and traveling outside the expectations consumers have regarding how companies will use their personal data.

Furthermore, the notice-and-consent model for privacy that currently predominates in unregulated industries in the United States has been roundly criticized as a failure.[24] Often taking the form of End User License Agreements (EULAs) or Terms and Conditions forms, these notices are prohibitively long and written in legalese that most consumers do not understand.[25] The result is that *no one* reads the terms and conditions for a given product or service.[26] Stories in recent news have demonstrated time and again that when faced with the prospect of read-

[21] Congress has chosen to focus on industry-specific laws to create standards for how data is handled. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C.A. § 1681 et seq. (Westlaw 2015) (credit information), Gramm-Leach-Bliley Act, 15 U.S.C.A. § 6801 et seq. (Westlaw 2015) (financial information); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–19145, 110 Stat. 1936 (codified as amended in scattered titles of U.S.C.) (medical information).

[22] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1880 (2013) ("Consent legitimizes nearly any form of collection, use, or disclosure of personal data.").

[23] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, DAEDALUS, J. AM. ACAD. ARTS & SCI., Fall 2011, at 32, 43–44.

[24] *E.g.*, *id.* at 32, 34; FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 2 (2012), *available at* www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 23 (2010), *available at* www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

[25] Nissenbaum, *supra* note 23, at 32, 35.

[26] Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read The Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 3 (2014) ("[O]nly one or two in 1,000 shoppers access a product's EULA for at least 1 second . . . .").

ing a lengthy EULA, consumers just agree and move on.[27] A comprehensive federal privacy law could address these concerns.

Additionally, the primary enforcer of privacy law, the Federal Trade Commission (FTC), does not have the capacity to enforce every privacy violation claim of which it is made aware.[28] While the FTC has an excellent track record of obtaining settlements with consumer privacy infringers, because of its limited budget it goes after only the biggest companies, leaving many smaller privacy infringements unremedied.[29] Even when the FTC does obtain a settlement, it does not require a company to admit to wrongdoing, and the settlement does not have the weight of precedent.[30]

This Comment will argue that there is a significant gap in federal privacy law that must be addressed. New federal legislation is needed to fill this gap and would be preferable to a mishmash of potentially conflicting state laws currently in development that will make compliance more difficult for companies that do business online.[31] The incorporeal nature of the Internet also cuts against relying on state legislation, because it makes it difficult to determine the proper jurisdiction for a claimed privacy violation, creating complex choice-of-law disputes.[32]

Furthermore, due to the intangible nature of PII, it is often difficult for plaintiffs to show damages from a privacy violation.[33] Without material damages to claim in a complaint, privacy plaintiffs have no standing to be in federal court.[34] A federal law providing a private right of action

[27] Rachel Feltman, *Londoners Accidentally Pay for Free Wi-Fi with a Firstborn, Because No One Reads Anymore*, WASH. POST, Sept. 29, 2014, www.washingtonpost.com/news/speaking-of-science/wp/2014/09/29/londoners-accidentally-pay-for-free-wi-fi-with-a-firstborn-because-no-one-reads-anymore (describing Wi-Fi terms and conditions clause that offered free Internet in exchange for the user's firstborn child); Larry Magid, *It Pays To Read License Agreements*, PC PITSTOP, www.pcpitstop.com/spycheck/eula.asp (last visited Apr. 20, 2015) (reporting that after 3,000 downloaders missed it, one man came forward to claim $1,000 cash prize hidden in EULA).

[28] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600 (2014).

[29] *Id.* (stating that the FTC averages around ten enforcement actions a year, although that number has been steadily increasing).

[30] *Cf. id.* at 620 (noting that privacy professionals nevertheless still treat FTC enforcement actions as having precedential weight).

[31] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 39 (2012), *available at* www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[32] The Internet has given rise to numerous disputes concerning international jurisdiction as well. For a discussion of choice-of-law issues arising from electronic contracts, see Aristotle G. Mirzaian, *Y2K Who Cares? We Have Bigger Problems: Choice of Law in Electronic Contracts*, 6 RICH. J.L. & TECH. 20 (2000).

[33] Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, *in* SECURING PRIVACY IN THE INTERNET AGE 111, 115 (Anupam Chander, Lauren Gelman & Margaret Jane Radin eds., 2008).

[34] *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).

for a mere violation is needed to keep privacy plaintiffs from being kicked out of federal courts on jurisdictional grounds. A new federal law providing a private right of action would strengthen consumers' confidence that their rights will be protected and encourage them to continue to participate in the developing digital economy, even as new technologies continue to make us more closely connected.

Part I of this Comment will describe how the concept of privacy has evolved over time, from its original constitutional conception to our modern informational conception. It will also discuss the self-regulation approach to privacy and its reliance on notice and consent. Part II will discuss the current state of federal privacy law and its shortcomings for a plaintiff attempting to bring a claim in federal court. Part III will describe the role of the FTC as the primary enforcer of privacy rights. Finally, Part IV will outline the features a new comprehensive federal online privacy law should embody.

I. THE EVOLUTION OF PRIVACY

In our modern hyper-connected world, the need for privacy protections is greater than it has ever been. However, our contemporary conception of privacy is somewhat different than it was when the word first came into common usage. In 1890, Samuel Warren and Louis Brandeis published their famous article, *The Right to Privacy*,[35] in response to the invention of the handheld camera.[36] They adapted Judge Cooley's "right to be left alone" phrase from his treatise on torts[37] and framed it for a larger audience as a new right.[38] They feared that as new technologies developed, a person's private life would require greater protection, thus necessitating a new right of privacy.

Warren and Brandeis's notion of privacy concerned decisional privacy, i.e., one's ability to make personal decisions without the intrusion of government or society at large. This conception is grounded in the idea that our constitutional guarantees create "zones of privacy" protecting the most intimate areas of life, such as the familial home.[39] This

[35] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[36] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 11 (4th ed. 2011) (discussing how Warren and Brandeis worried about the contemporary media of their day).

[37] THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (2d ed. 1888).

[38] Harry Kalven, Jr., *Privacy in Tort Law–Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 327 (1966) (stating that Warren and Brandeis article is likely the "most influential law article of all").

[39] *See, e.g.*, Payton v. New York, 445 U.S. 573, 589–90 (1980); Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965).

conception should be distinguished from informational privacy, in that the latter is concerned with the protection of personal details rather than being left alone.

Consumers are now sharing more information than ever, and that data must be protected. In Warren and Brandeis's time, it was likely unthinkable how much personal information would be stored about each person in the technological age. Decisional privacy is still important, but the sheer volume of personal data in cyberspace means that informational privacy has taken center stage for the average consumer.

In 1960, seventy years after Warren and Brandeis wrote their article, William Prosser organized the concept of invasion of privacy into four distinct torts: intrusion upon seclusion, public disclosure of private facts, false light, and appropriation of likeness.[40] The four-tort scheme he devised imposed an order on privacy law, but that order also gave privacy law a rigidity it did not previously have.[41] It resulted in privacy law being unable to adapt to new changes in technology or developments in contemporary culture.[42] For example, these torts are not equipped to deal with informational privacy, because they are concerned with a person's "interest in solitude."[43] This is inapposite to many common instances nowadays, such as when a consumer reaches out and furnishes his or her personal information to a company in order to receive goods and services. Privacy concerns have shifted from wanting to "be left alone," to wanting to feel that personal information is secure in the hands of companies who hold it. There is a need for legislation that can adequately address the intricacies of how consumers expect their information to be handled. This requires a subtlety that the four original privacy torts are unable to furnish.[44]

In addition, the tort model of privacy causes courts to look for concrete injury in a privacy case for which to award damages. However, due to the nature of privacy claims, this is often an impossible task.[45] When a company fails to follow its own privacy policy and shares a consumer's personal information without permission, there is no con-

[40] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

[41] *See generally* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010).

[42] *Id.* at 1890.

[43] RESTATEMENT (SECOND) OF TORTS § 652B cmt. a (1977).

[44] Richards & Solove, *supra* note 41, at 1921.

[45] Solove, *supra* note 33, at 115–16 (observing that concrete harms from a privacy infringement may not appear for years, which makes proving a causal connection very difficult).

crete damage to the information.[46] However, that does not mean that the consumer has not been harmed.

In regulating privacy online, the United States has preferred to let businesses take a self-regulation approach.[47] Self-regulation is considered the "least intrusive and most efficient means" to use in such a rapidly evolving area as the Internet.[48] This approach relies on notice and consent, whereby a company is required to provide notice to consumers of how it will collect and use their information, and consumers consent by using the goods or services the company provides.[49] Ideally, the notice-and-consent system allows market forces to dictate in a flexible way which privacy practices consumers find most agreeable, without the need for paternalistic regulatory oversight.[50]

However, notice-and-consent is broken.[51] The current way companies provide notice, usually through privacy policies or terms-of-service agreements, is not an effective method of informing consumers about impacts to their privacy.[52] It would take a prohibitively long time to read even a fraction of the privacy policies a consumer may encounter online in a given day.[53] In addition, it is nearly impossible for consumers to weigh the convenience of using a company's services against the long-term effects to their privacy stemming from the myriad ways a company may use their personal information.[54] The result is that consumers do not read privacy policies, and if they do, they do not understand them. Thus, the checks and balances that the notice-and-consent system was designed to provide have failed to materialize.[55]

---

[46] *See, e.g.*, *In re* Google Android Consumer Privacy Litig., No. 11-MD-02264 JSW, 2013 WL 1283236, at *4 (N.D. Cal. Mar. 26, 2013) (finding that Google's covert collection of plaintiffs' PII resulted in no diminution of it's value).

[47] FTC, SELF REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 6 (1999), *available at* www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf.

[48] *Id.* ("[S]elf-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology.").

[49] Felix T. Wu, *The Constitutionality of Consumer Privacy Regulation*, 2013 U. CHI. LEGAL F. 69, 71 (2013) (describing "notice and choice" instead of "notice and consent").

[50] Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 929 (2013).

[51] *E.g.*, Nissenbaum, *supra* note 23, at 32, 34; FTC, *supra* note 24, at 2; DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, *supra* note 24, at 23.

[52] Wu, *supra* note 49, at 71.

[53] *Id.*

[54] *Id.*

[55] Bakos et al., *supra* note 26, at 3 ("[O]nly one or two in 1,000 shoppers access a product's EULA for at least 1 second . . . ."); Feltman, *supra* note 27 (describing Wi-Fi terms and conditions clause that offered free Internet in exchange for the user's firstborn child).

II. CURRENT FEDERAL PRIVACY LEGISLATION[56]

The Privacy Act of 1974 represented the first attempt by Congress to address privacy concerns.[57] At that time, social security numbers were still in wide use by government organizations to provide access to user accounts.[58] Congress drafted the Privacy Act in order to limit the use of social security numbers because "common numerical identifiers" do not make secure passwords.[59] However, in drafting the Act, Congress made it applicable only to government agencies, thus allowing all private use of social security numbers to escape the enforcement of the Act.[60]

The advent of the Internet again changed the way we conceive of privacy. In the early days of the Internet, Congress passed the Wiretap Act[61] and the Stored Communications Act[62] as part of the Electronic Communications Privacy Act of 1986 (ECPA).[63] However, the Act was drafted when much of the technology making up the Internet was still evolving, and it has become clearly inadequate for the ways consumers now use the Internet to email, engage in social networks, and shop.[64]

For example, the ECPA distinguishes between real-time communications and stored records, providing reduced protections for the latter.[65] This made sense when storing electronic materials was prohibitively expensive, simply because it was so uncommon that it presented a lower risk than that posed by real-time interceptions.[66] In the present day, however, server storage is so cheap that is common to retain all emails a consumer has ever received, or in the case of Facebook, every click a user has ever made while using its site.[67] In addition, now that cloud computing allows consumers to share private content across multiple devices, the reduced protection provided to stored data puts much more

[56] This Comment is not intended to be an exhaustive treatment of available federal privacy legislation. It instead offers a sampling of laws being used by consumers to protect their privacy in order to show the laws' deficiencies, and the need for new comprehensive legislation.

[57] 5 U.S.C.A. § 552a (Westlaw 2015).

[58] Doyle v. Wilson, 529 F. Supp. 1343, 1348 (D. Del. 1982).

[59] *Id.* (pointing out the dangers created by requiring citizens to disclose their social security numbers for use as passwords).

[60] Solove, *supra* note 33, at 120.

[61] 18 U.S.C.A. § 2510 et seq. (Westlaw 2015).

[62] *Id.* § 2701 et seq.

[63] Electronic Communications Privacy Act (ECPA), Pub. L. No. 99–508, 100 Stat. 1848 (1986).

[64] *See generally* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 390–411 (2014) (discussing how changes in the technologies that make up the Internet have made the ECPA outdated).

[65] *Id.* at 390–91.

[66] *Id.*

[67] *Id.* at 391–93.

content at risk. This has resulted in a paradigm in which stored communications can now tell much more about a person than information disclosed in real time, because stored communications have the potential to include all of a person's online activity going back decades.[68] Now that technology has broken down the wall between real-time communications and stored records, there should be an equal level of protection for personal information regardless of its temporal status.

An additional outdated feature of the ECPA is its reliance on the distinction between providers of Electronic Communications Service (ECS)[69] and Remote Computing Service (RCS).[70] The ECS protections covered email, and the RCS protections covered "contents of communications transmitted for remote storage and processing by services available to the public."[71] If content falls within neither of these categories it is not protected under the Act.[72] In 1986 this dichotomy made sense, but modernly it leaves many aspects of the Internet unprotected, such as search queries.[73] Additionally, many service providers on the Internet today perform multi-functional roles, such as messaging, chat, photograph hosting, and bulletin board services.[74] Relying on the Act to protect content held by these multi-functional providers means that content consumers share with a single provider will be afforded varied levels of protection based on whether the provider is acting as an ECS or RCS with regard to that specific content at the relevant time.[75] It is time to let go of this old dichotomy, which has been outpaced by technology and no longer reflects the nature of the Internet.

Another way that the ECPA is ill-equipped to handle the current state of the Internet is its failure to tackle the problem of territoriality.[76] The ECPA was drafted before the advent of the World Wide Web, and as such it does not address the fact that data can now be transferred to or stored in just about any country in the world.[77] It is now common for a company headquartered in the United States to have customers in Europe

[68] *Id.* at 393.

[69] 18 U.S.C.A. § 2510(15) (Westlaw 2015) ("'[E]lectronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications.").

[70] *Id.* § 2711(2) ("'[R]emote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.").

[71] Kerr, *supra* note 64, at 395.

[72] *Id.*

[73] *Id.* at 395–96 ("ECPA likely offers no protection for access to stored search queries, however, because it does not fit the 1986 dichotomies codified by the statute.").

[74] *Id.* at 397 (providing Facebook as an example of a service provider that wears many hats).

[75] *Id.* at 397–98.

[76] *Id.* at 406.

[77] *Id.*

and its servers in Asia. The Act provides no answers for whose laws or what factors should control how the data is handled, whether it is the location of the data, the location of the business holding it, or the location of its sender or receiver.[78] The truly global nature of the Internet requires that for any new federal privacy legislation to be effective, it must address how data is handled in the international context.

The current administration has stated its interest in updating the Wiretap Act to coincide with the modern realities of Internet use,[79] but so far Congress has failed to do so. Congress has chosen to focus instead on crafting industry-specific laws[80] and has left it up to the states to develop a "hodgepodge" of privacy laws.[81] This can make compliance difficult for companies that seek to do business online,[82] and it offers residents of different states fluctuating levels of privacy protection.[83]

Although the Wiretap Act is outdated, plaintiffs frequently assert claims under the Act for violations of their informational privacy.[84] This is likely due, at least in part, to the fact that the statute does not require plaintiffs to show damage arising out of the alleged violations of their privacy.[85] This allows privacy plaintiffs to overcome a difficult hurdle, as there are frequently no concrete harms for courts to latch onto in privacy claims.[86]

[78] *Id.* at 407–08.

[79] WHITE HOUSE, *supra* note 31, at 35 n.42 ("The Administration is separately considering the need to amend laws pertaining to the government's access to data in the possession of private parties, including the Electronic Communications Privacy Act, to address changes in technology.").

[80] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C.A. § 1681 et seq. (Westlaw 2015); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (codified as amended in scattered titles of U.S.C.).

[81] Glancy, *supra* note 17, at 359 n.6.

[82] WHITE HOUSE, *supra* note 31, at 39.

[83] For a thorough treatment of state privacy laws, see generally Jonathan D. Frieden, Charity M. Price & Leigh M. Murray, *Putting the Genie Back in the Bottle: Leveraging Private Enforcement To Improve Internet Privacy*, 37 WM. MITCHELL L. REV. 1671 (2011).

[84] *See, e.g.*, *In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1071–72 (N.D. Cal. 2011) (noting that plaintiffs alleged violations of ECPA when Google intercepted usernames, passwords, and emails from their wireless networks with its street view cars equipped with "packet sniffers"); *In re* Facebook Privacy Litig., 791 F. Supp. 2d 705, 712–13 (N.D. Cal. 2011) (noting that plaintiffs alleged violation of the Wiretap Act when Facebook shared their personal information with third-party advertisers); *In re* Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 316 (E.D.N.Y. 2005) (noting that plaintiffs alleged violations of ECPA due to airline disclosing passenger information to a third party); Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196 (D.N.D. 2004) (same); *In re* Nw. Airlines Privacy Litig., No. Civ.04-126(PAM/JSM), 2004 WL 1278459 (D. Minn. June 6, 2004) (same).

[85] 18 U.S.C.A. § 2520 (Westlaw 2015).

[86] *See, e.g.*, Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477, 486 (2010) (bringing attention to the fact that tort law in America looks for harms that can be expressed in monetary amounts).

Standing is a jurisdictional prerequisite, and so a federal court will be quick to dismiss a claim for lack of standing if the plaintiff is unable to show injury from an alleged privacy violation.[87] For a plaintiff to have standing, he or she must show "(1) [he or she 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."[88] Privacy plaintiffs often run afoul of the standing test in that without monetary damage arising from their privacy violations, they are unable to demonstrate they have suffered "injury in fact" that is "concrete and particularized."[89] However, it is still possible to get standing from a statute such as the ECPA, which provides a remedy without requiring a separate showing of damages.[90]

Without such a statute, even when a plaintiff has suffered economic harm as a result of trying to mitigate an anticipated future privacy violation, the Supreme Court has held that such an injury is too speculative for standing.[91] In *Clapper v. Amnesty International USA*, the Court held that plaintiffs could not "manufacture standing" based on their fears of a speculative future harm and the money they spent in order to safeguard against surveillance of their client communications.[92] This strict reading of the imminence requirement for standing further restricts the situations in which a privacy plaintiff may bring a claim absent a showing of an imminent violation.

[87] FW/PBS, Inc. v. City of Dallas, 493 U.S. 215, 231 (1990).

[88] Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000) (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61).

[89] *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646 (S.D. Ohio 2014) (finding plaintiffs had no standing even though their personal information was hacked from the insurance carrier, because there was no evidence they had suffered economic harm as a result); *In re* Google Android Consumer Privacy Litig., No. 11–MD–02264 JSW, 2013 WL 1283236 (N.D. Cal. Mar. 26, 2013) (finding Google's collection of PII without disclosure or consent did not result in sufficient diminution in value to establish standing); Rudgayzer v. Yahoo! Inc., No. 5:12–CV–01399 EJD, 2012 WL 5471149 (N.D. Cal. Nov. 9, 2012) (finding plaintiff had no standing because he could not show that Yahoo's disclosure of his personal information caused him to suffer harm); Cherny v. Emigrant Bank, 604 F. Supp. 2d 605 (S.D.N.Y. 2009) (finding plaintiffs had no standing because they could show no injury beyond the receipt of spam from the bank's disclosure of customer information in violation of its own privacy policy).

[90] Warth v. Seldin, 422 U.S. 490, 500 (1975) ("The actual or threatened injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing . . . ." (internal quotation marks omitted)).

[91] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148–50 (2013) (finding plaintiffs challenging a provision of the Foreign Intelligence Surveillance Act did not have standing because it was only speculative that the government would target them for surveillance).

[92] *Id.* at 1151.

Conversely, a plaintiff seeking to bring a claim under the Wiretap Act merely has to demonstrate that the statute was violated.[93] This feature of the Act allows privacy plaintiffs to sidestep the standing hurdle, but the poor fit of the statute to the modern Internet means that even if a plaintiff gains standing through the ECPA, often he or she will not have a claim under the Act.[94]

One of the first cases in which private plaintiffs asserted a violation of the ECPA was *In re Doubleclick Inc. Privacy Litigation*.[95] In that case, the plaintiffs contended that Doubleclick Inc., a targeted advertising company, used "cookies" to track them online and compile voluminous consumer profiles based on the sites they visited, in violation of the ECPA.[96] However, Doubleclick tracked consumers only when they visited sites affiliated with Doubleclick, i.e., sites that used Doubleclick's targeted ad banners.[97] For that reason, the court held Doubleclick's use of cookies did not violate the Wiretap Act, because one of the parties of the tracked communication, the affiliated website, obviously consented to the use of cookies when it chose to utilize Doubleclick's services.[98] Therefore, the cookies fell under the exception to the Wiretap Act that applies when one party to a communication consents to a third party's access.[99]

Doubleclick was notable because it allowed interception of consumers' personal information without their consent. It stands for the proposition that a third party may collect the PII a consumer enters into a given site, as long as *the site* consents to the acquisition.[100]

In a more recent case, *In re Facebook Privacy Litigation*, plaintiffs attempted to use the ECPA to claim that Facebook violated their infor-

[93] *In re* iPhone Application Litig., No. 11–MD–02250–LHK, 2011 WL 4403963, at *6 (N.D. Cal. Sept. 20, 2011) ("[S]tatutory standing under the Wiretap Act does not require a separate showing of injury, but merely provides that any person whose electronic communication is intercepted, disclosed, or intentionally used in violation of the Act may in a civil action recover from the entity which engaged in that violation." (internal quotation marks omitted)).

[94] *See, e.g.*, *In re* Facebook Privacy Litig., 791 F. Supp. 2d 705, 713 (N.D. Cal. 2011) (finding plaintiffs had no claim under ECPA because the advertisers were a party to the communication); Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004) (finding plaintiffs had no claim under ECPA because airline was not an "electronic communications service" provider); *In re* Nw. Airlines Privacy Litig., No. Civ.04-126(PAM/JSM), 2004 WL 1278459, at *2 (D. Minn. June 6, 2004) (same); *In re* Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 306–07, 310 (E.D.N.Y. 2005) (finding plaintiffs had no claim under ECPA because airline was not an "electronic communications service" provider nor a "remote computing service" provider).

[95] *In* re Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[96] *Id.* at 502.

[97] *Id.* at 504.

[98] *Id.* at 510.

[99] *See* 18 U.S.C.A. § 2701(c)(2) (Westlaw 2015) (providing for exceptions to the Act when authorized by a user of the service in question).

[100] *In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d at 510, 514.

mational privacy through its disclosure to third-party advertisers.[101] The complaint focused on users who clicked banner ads they were shown in Facebook.[102] When users clicked the ads, Facebook would send personally identifiable information about the users to third-party advertisers.[103]

The court found that Facebook's actions did not violate the ECPA, because by clicking the advertisements either the users were contacting the advertiser, or they were contacting Facebook to pass their interest on to the advertiser.[104] The court determined that under either theory Facebook's actions fell under a consent exception to the ECPA, because when users clicked on the banner ads they were attempting to communicate with the advertisers.[105] Thus, the advertisers were the intended recipients of the communication, and Facebook was authorized to send them user data.[106]

In re Facebook is unsettling, because the court did not appear to consider the *amount* of user information that Facebook sent to the advertisers, only that it *could* send user information to the advertisers. This fails to take into account the context-based expectations of users that their personal information will not be shared with third-party advertisers merely because they click on advertisements.[107]

The cases looked at thus far have demonstrated that the ECPA often leaves plaintiffs without cognizable claims when they allege violations of their informational privacy. In the last two cases, plaintiffs were concerned about defendant activity that went beyond their reasonable expectations under the circumstances. Although it appears that the plaintiffs did in fact suffer violations of their privacy, the ECPA was not the right vehicle for them to use for litigation. Although the ECPA helped them get standing, it did not assist them to state a claim or obtain relief.

In contrast to the plaintiffs above, the FTC has been very successful in bringing actions against companies it has determined were behaving in an unfair or deceptive manner. While the FTC's record with consent decrees has been very influential in the privacy community, it is not without certain drawbacks. The next Part will analyze the FTC's role in privacy enforcement.

---

[101] *In re* Facebook Privacy Litig., 791 F. Supp. 2d 705 (N.D. Cal. 2011).

[102] *Id.* at 711.

[103] *Id.* at 713.

[104] *Id.*

[105] *Id.*

[106] *See* 18 U.S.C.A. § 2511(3)(a) (Westlaw 2015) ("[A] person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (*other than one to such person or entity, or an agent thereof*) . . . ." (emphasis added)).

[107] *See generally* Nissenbaum, *supra* note 23, at 32.

III. THE FTC'S ROLE

In the large hole left by the absence of any comprehensive online federal privacy law, the FTC[108] has become the de facto privacy regulator for the federal government.[109] The FTC enforces consumers' online privacy by targeting companies that engage in unfair competition and deceptive practices, as defined in section 5 of the FTC Act.[110] The FTC also brings complaints against companies that have self-certified as Safe Harbors[111] under the U.S.-EU framework.[112] While the FTC has a near-perfect record of obtaining a consent order once it brings a complaint against a company,[113] its relatively small staff of personnel and limited budget restricts the number of complaints it can bring in any given year.[114] Despite this limitation, the FTC Act does not provide a private cause of action for consumers to bring their own claims against those who have violated their privacy rights.[115] Even so, the strategies the FTC has developed to bring complaints against violators will be useful to consider in developing new federal privacy legislation.

[108] FED. TRADE COMMISSION, www.ftc.gov (last visited Apr. 20, 2015). The FTC keeps a record on its website of all the cases it has initiated thus far. They can be found by accessing the "cases and proceedings" heading under the "enforcement" tab found on the main page. In addition, the International Association of Privacy Professionals has released a casebook of FTC Privacy Law that summarizes, organizes, and tags all the FTC settlements to date to make them easier to search. *FTC Privacy Casebook*, IAPP WESTIN RESEARCH CTR., www.privacyassociation.org/resources/ftc-casebook (last visited Apr. 20, 2015).

[109] WHITE HOUSE, *supra* note 31, at 29.

[110] 15 U.S.C.A. § 45 (Westlaw 2015).

[111] Complaint at 17–18, *In re* Facebook Inc., File No. 092-3184, No. C-4365 (F.T.C. July 27, 2012) ("The U.S.-EU Safe Harbor Framework provides a method for U.S. companies to transfer personal data outside of the European Union ('EU') that is consistent with the requirements of the European Union Data Protection Directive ('Directive'). The Directive sets forth EU requirements for privacy and the protection of personal data. . . . To join the Safe Harbor, a company must self-certify to Commerce that it complies with seven principles and related requirements that have been deemed to meet the EU's adequacy standard.").

[112] *See, e.g.*, *id.* at 17–19 (stating Facebook's retroactive change of users' privacy settings without obtaining consent constituted a deceptive practice, and as such did not comply with the Safe Harbor requirements of notice and choice); Complaint at 6–8, *In re* Google, File No. 102-3136, No. C-4336 (F.T.C. Oct. 13, 2011) (stating Google's use of Gmail user information in the Google Buzz social media platform without first providing notice and obtaining consent constituted a deceptive practice, and as such did not comply with the Safe Harbor requirement of choice).

[113] Solove & Hartzog, *supra* note 28, at 606.

[114] *Id.* at 600.

[115] *Id.* at 610. To make up for the FTC's limited size, state attorneys general are also authorized to bring complaints for unfair and deceptive practices, but this Comment will not discuss their role, because it is concerned with creating a comprehensive federal legislation that empowers private plaintiffs to defend themselves against privacy violations. This Comment argues that a single comprehensive federal privacy law would be superior in that it would foster consumer confidence and allow for greater ease of compliance by businesses in the national and international context.

Chief among the FTC's arsenal is the power to bring complaints against companies that engage in unfair or deceptive business practices.[116] Unfair business practices may include retroactively changing a company's privacy policy without notifying users or giving them the choice to opt out, collecting user data without notice, or implementing substandard security procedures.[117] A deceptive business practice may consist of a company sharing user information with third-party advertisers despite stating previously that it would never do so without user notification,[118] or a company illicitly collecting personal information from consumers.[119] The FTC must weigh an alleged unfair practice against any countervailing benefits to consumers resulting from the practice.[120] Only if the FTC finds there is a substantial injury to consumers, and no comparable benefit to consumers, may it bring a complaint for unfairness against a company.[121] Thus, there have been many more complaints alleging deception than unfairness.[122]

Utilizing these two principles, the FTC has developed a robust record of settlements that privacy professionals pay close attention to in order to determine best practices in the area of informational privacy.[123] While settlements do not set precedent, their influence in the professional privacy community means that companies treat consent orders much like judicial decisions that have the weight of precedent.[124] This is true even though consent orders do not require companies to admit to any wrongdoing.[125] An added benefit of settling is efficiency, in that the FTC and the company in question do not have to tie up the courts and spend vast sums of money in litigation.

---

[116] 15 U.S.C.A. § 45 (Westlaw 2015).

[117] Solove & Hartzog, *supra* note 28, at 628 ("[U]nfairness actions are based on at least five distinct theories: retroactive policy changes, deceitful data collection, improper use of data, unfair design, and unfair information security practices.").

[118] *See, e.g.*, Complaint at 11–14, *In re* Facebook Inc., File No. 092-3184, No. C-4365 (F.T.C. July 27, 2012).

[119] Solove & Hartzog, *supra* note 28, at 628 ("The FTC has developed a theory of deception that not only includes broken promises of privacy and security, but also a general theory of deception in obtaining personal information and deception due to insufficient notice of privacy-invasive activities.").

[120] *Id.* at 638 (describing the "three-part test" for FTC unfairness actions).

[121] *See* 15 U.S.C.A. § 45(n) (Westlaw 2015).

[122] Solove & Hartzog, *supra* note 28, at 628 n.211 ("Of the 154 privacy-related complaints analyzed for this Article, eighty-seven unambiguously relied upon a theory of deception in alleging a violation of Section 5 [of the FTC Act, 15 U.S.C. § 45], whereas there were only forty-six complaints that unambiguously relied upon a theory of unfairness in alleging a violation of Section 5.").

[123] *Id.* at 607.

[124] *Id.* at 621–622.

[125] *See, e.g.*, Decision and Order at 1, *In re* Designerware, LLC, File No. 112-3151, No. C-4390 (F.T.C. 2013) ("[T]he signing of said consent agreement is for settlement purposes only and does not constitute an admission by the respondent that the law has been violated . . . .").

However, the FTC is limited to seeking equitable relief for most violations of the FTC Act.[126] This means that often companies get away without paying any fines or damages. On the other hand, the FTC has made a habit of imposing twenty-year audit periods in its consent orders,[127] with the audits to be conducted by qualified third parties, which are their own unique burden and a long time to be under the watchful eye of the FTC.[128] The consent orders, in addition to requiring regular audits, also impose hefty civil fines if they are violated. Google was recently found to have violated its 2011 Google Buzz consent order by making misrepresentations to Safari users about placement of cookies on the Safari web browser, and it was fined $22.5 million, the largest fine the FTC has obtained for a violation of one of its orders to date.[129]

In addition to its deceptive-practice authority, the FTC also can bring complaints against companies for violation of the U.S.-EU Safe Harbor principles.[130] A company that holds itself out as a safe harbor claims that it upholds the seven privacy principles included in the European Union Data Protection Directive.[131]

Because a company must self-certify as a safe harbor, if the FTC determines that a company has not upheld the seven principles, it can also bring a complaint for deceptive practice in that the company held

---

[126] 15 U.S.C.A. § 53(b) (Westlaw 2015).

[127] *See, e.g.*, Decision and Order at 8, *In re* Facebook, Inc., File No. 092-3184, No. C-4365 (F.T.C. July 27, 2012); Decision and Order at 7, *In re* Google, Inc., File No. 102-3136, No. C-4336 (F.T.C. Oct. 13, 2011); Decision and Order at 6, *In re* Myspace LLC, File No. 102-3058, No. C-4369 (F.T.C. Aug. 30, 2012); Decision and Order at 6, *In re* Twitter, Inc., File No. 092-3093, No. C-4316 (F.T.C. Mar. 2, 2011).

[128] As part of its twenty-year audit period, the FTC often requires companies to institute new comprehensive privacy programs to address continuing and developing privacy risks. *See, e.g.*, Decision and Order at 4–5, *In re* Facebook, Inc., File No. 092-3184, No. C-4365.

[129] Press Release, Fed. Trade Comm'n, Statement by FTC Bureau of Consumer Protection Director David Vladeck Regarding Judges Approval of Google Safari Settlement (Nov. 20, 2012), *available at* www.ftc.gov/news-events/press-releases/2012/11/statement-ftc-bureau-consumer-protection-director-david-vladeck.

[130] Solove & Hartzog, *supra* note 28, at 643, 647–48.

[131] *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated Dec. 18, 2013) (listing the seven principles as notice (telling consumers what personal information is collected and for what purposes it is used), choice (allowing consumers to opt out of transfer to third parties or the use of information for secondary purposes, and requiring opt-in for sensitive information), transfers to third parties (requiring that the third party maintain a similar level of privacy protection), access (allowing consumers to check their data for accuracy and to correct or delete it), security (maintaining reasonable security measures for data to guard against loss or unauthorized access), data integrity (taking reasonable steps to ensure consumer data is reliable and accurate), and enforcement (maintaining mechanisms for individual complaints and procedures for ensuring compliance with the above principles)).

itself out as maintaining a certain level of privacy protection that it did not actually provide.[132]

While the FTC settlement history is impressive and expansive, it suffers from several deficiencies. First, the FTC may use its administrative authority only against companies engaging in unfair or deceptive practices.[133] If a company provides notice to consumers in its terms of service for wildly out-of-context sharing of personal information, the FTC is powerless to bring an action against it.[134] Second, because companies choose to settle with the FTC instead of going to trial, there is no privacy precedent being created by courts.[135] This results in only privacy professionals studying the terms of the settlements, with most consumers being unaware of the current state of FTC privacy law. Furthermore, while privacy professionals may treat FTC orders as precedential for practical purposes, there is nothing preventing the FTC from changing its standards at any time. Third, companies that settle with the FTC are not required to admit any wrongdoing, and so they escape the reputational damage they may otherwise incur from adverse court judgments. This reduces their incentive to get privacy right the first time around. Fourth, because the FTC cannot impose statutory fines as a penalty, companies have the potential to profit enormously from violating consumer privacy while having to repay only a small amount. Even when Google was fined $22.5 million for violating its consent order, the stiffest penalty the FTC has imposed thus far, the fine was a drop in the bucket compared to the over $50 billion Google made in revenue that same year.[136] Finally, the FTC Act does not provide a private cause of action for consumers whose privacy is violated. If the FTC does not consider a company's violations to be worth the trouble to begin proceedings against it, consumers are left with no remedy. A new federal privacy law could remedy these deficiencies by empowering consumers to seek redress for violations of their privacy by embodying the same principles the FTC uses to obtain its settlements.

---

[132] *See, e.g.*, Complaint, *In re* Progressive Gaitways LLC, File No. 092-3141, No. C-4271 (F.T.C. Nov. 9, 2009).

[133] 15 U.S.C.A. § 45 (Westlaw 2015).

[134] Solove, *supra* note 22, at 1880 ("Consent legitimizes nearly any form of collection, use, or disclosure of personal data.").

[135] *Cf.* Solove & Hartzog, *supra* note 28, at 619–20 (noting that while the FTC's consent decree settlements do not technically create precedent, they are treated as having precedential power by privacy professionals).

[136] *Google Inc. Announces Fourth Quarter and Fiscal Year 2012 Results*, GOOGLE INVESTOR RELATIONS (Jan. 22, 2013), http://investor.google.com/earnings/2012/Q4_google_earnings.html.

IV. Proposed Federal Legislation

A new federal privacy law should utilize the experience the FTC has gained through its settlements to provide consumers with a private right of action for violations of their privacy. An ideal law would also utilize the "Fair Information Practice Principles" of transparency, notice, control, access, and security to require companies to maintain a new minimum level of privacy protection.[137] The FTC has recommended multiple times that new privacy legislation be enacted to embody these principles and make them applicable to any business that collects consumer personal data online.[138] Further, new legislation should create a standard based on reasonable consumer expectations (based on context), holding accountable any company that collects, uses, processes, discloses, or stores personally identifiable information. In addition, the legislation should provide a private right of action based on a violation of any of its provisions, without requiring a separate showing of harm by a plaintiff. The Obama Administration recently released a proposed bill, the "Consumer Privacy Bill of Rights Act of 2015," which included many of these principles.[139] Notably absent from the bill, however, was a private right of action.

The benefits of new legislation are readily apparent. Giving consumers a private right of action without having to show damages would allow more privacy violations to be remedied in court. This would create a new wave of judicial precedent, a necessary feature of our common-law system. It would also result in improved transparency of corporate practices, as businesses would have an increased incentive to demonstrate their compliance with the new legislation. Additionally, the updated legislation would save plaintiffs from trying to force their arguments to fit outdated statutes, or from relying on negligence theories for recovery, where proving causation and damages in privacy cases is

[137] U.S. Dep't of Health, Educ. & Welfare, Records, Computers, and the Rights of Citizens 38–42 (1973), *available at* www.justice.gov/opcl/docs/rec-com-rights.pdf (originally describing the Fair Information Practice Principles). The FIPPs were later expanded by the Organization for Economic Cooperation and Development (OECD) to include eight principles. Org. for Econ. Cooperation & Dev., Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980).

[138] FTC, *supra* note 24, at 12–13; FTC, Privacy Online: Fair Information Practices in the Electronic Marketplace 36–37 (2000), *available at* www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf.

[139] Office of Mgmt. & Budget, Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, *available at* www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

difficult.[140] Furthermore, the new legislation would ideally provide for statutory damages, which would serve as a deterrent to companies that otherwise may not take privacy protection seriously and would allow potential plaintiffs to recover for the aggravation suffered due to having their privacy violated.

In the Target credit card breach example that began this Comment, consumers who want to bring lawsuits will be forced, in the absence of existing federal privacy legislation, to center their complaints on claims of negligence by Target or violations of state consumer protection statutes. This means that plaintiffs in different states may receive varying levels of protection from their state statutes. This will also limit the damages to which they will be entitled, because they may not be able to show any concrete harm resulting from their stolen credit card numbers beyond the cost of credit-monitoring programs.[141] This will do nothing to compensate them for the aggravation that results from having to deal with potential identity theft, unless it rises to the level that a court will be willing to recognize. New privacy legislation could provide victims of the Target breach with a clear right of action based on Target's alleged failure to maintain sufficient security procedures for their personal data. This would also allow them to seek compensatory and punitive damages resulting from the breach.[142]

Similarly, plaintiffs from *In re Facebook Privacy Litigation*[143] could have used new privacy legislation to claim that Facebook's broken promise not to share user data with advertisers constituted a deceptive act that violated the principles of notice and choice. Instead of having their claims dismissed, they could have recovered for Facebook's disregard for their informational privacy.

While the FTC settlement with Facebook served to prevent that sort of retroactive policy changing and promise breaking, it did not put remedial funds in the hands of individual users. Although Facebook profited by selling user information to advertisers in violation of its policy, the

[140] Solove, *supra* note 33, at 115–16.

[141] *Id.*

[142] As of Mar. 18, 2015, the consumer plaintiffs to the Target breach class action lawsuit have arrived at a proposed settlement agreement with Target, now awaiting final approval, in the amount of $10 million. Settlement Agreement and Release at 7, *In re* Target Corp. Customer Data Sec. Breach Litig., No. 14-2522 (PAM/JJK) (D. Minn. Mar. 18, 2015), *available at* https://targetbreachsettlement.com/Portals/0/Documents/Settlement%20Agreement.pdf. To obtain actual "reimbursement of losses" up to $10,000, class members must be able provide documentation of losses they incurred from the breach. *Detailed Notice*, TARGET BREACH SETTLEMENT, *available at* https://targetbreachsettlement.com/Portals/0/Documents/DetailedNotice.pdf (last updated Apr. 30, 2015). However, class members who file valid claims under the settlement without documentation will only be entitled to a general share of the settlement, which may be as little as $30. *Id.*

[143] *In re* Facebook Privacy Litig., 791 F. Supp. 2d 705 (N.D. Cal. 2011).

users themselves received nothing in compensation for the violation of their privacy rights. New legislation could remedy this situation by providing for recovery by users.

Accountability should also be a key feature of any new federal privacy legislation.[144] The Centre for Information Policy Leadership has listed the essential elements of accountability:

1. Organisation commitment to accountability and adoption of internal policies consistent with external criteria.
2. Mechanisms to put privacy policies into effect, including tools, training and education.
3. Systems for internal, ongoing oversight and assurance reviews and external verification.
4. Transparency and mechanisms for individual participation.
5. Means for remediation and external enforcement.[145]

The accountability principles listed above bear a strong similarity to FTC settlements requiring companies to institute comprehensive privacy programs.[146] The elements of accountability essentially require a company that collects personally identifiable data to demonstrate a commitment to privacy principles and create a robust program that provides a comprehensive scheme for carrying out those principles.[147] While this is a higher bar than exists currently, there are many companies that already meet this standard.[148] In addition, adoption of the accountability principles in federal legislation will bring the United States more in line with the privacy laws of other developed countries—a laudable objective, as the Internet does not function by normal jurisdictional rules or physical boundaries, and many companies are international in scope.[149] Further-

[144] THE CENTRE FOR INFO. POLICY LEADERSHIP, DATA PROTECTION ACCOUNTABILITY: THE ESSENTIAL ELEMENTS 3–4 (2009), *available at* www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf. The Centre for Information Policy Leadership defines accountability as: "shift[ing] the focus of privacy governance to an organisation's ability to demonstrate its capacity to achieve specified privacy objectives. It involves setting privacy protection goals for companies based on criteria established in law, self-regulation and best practices, and vesting the organisation with both the ability and the responsibility to determine appropriate, effective measures to reach those goals. . . . An accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised external criteria, and implements mechanisms to ensure responsible decision-making about the management and protection of data." *Id.*

[145] *Id.* at 4.

[146] *See, e.g.*, Decision and Order at 4–5, *In re* Facebook, Inc., File No. 092-3184, No. C-4365 (F.T.C. 2012).

[147] THE CENTRE FOR INFO. POLICY LEADERSHIP, *supra* note 144, at 8–9.

[148] *Member Companies*, CENTRE FOR INFO. POL'Y LEADERSHIP, www.informationpolicycentre.com/member_companies (last visited April 20, 2015).

[149] THE CENTRE FOR INFO. POLICY LEADERSHIP, *supra* note 144, at 7. The EU's Organisation for Economic Co-operation and Development (OECD), Canada's Personal Information Protection

more, the FTC already incorporates accountability principles into its consent orders, demonstrating that federal regulators consider accountability to be vital to privacy protection.

CONCLUSION

Any company that makes a profit from the collection of personally identifiable information should be tasked with the proper use, storage, and disposal of that information. New federal privacy legislation could accomplish this task by requiring companies to maintain adequate standards to safeguard this information utilizing the principles described above, with power given to private plaintiffs to enforce those principles if they are violated.

The current sectorial framework focuses on a select few industries and leaves large swaths of Internet activity without statutory protection. This system relies on self-regulation by companies, leaving the FTC and state attorneys general to bring enforcement actions against the largest infringers. However, the limited resources of the FTC, along with differing state privacy laws, mean that consumers receive varied levels of protection from national and international companies. These same companies must also find ways to conform and adapt to differing standards in the absence of comprehensive federal privacy legislation.

The Obama Administration, regulators, businesses, and consumers all support new federal legislation.[150] In order to maintain the strength of the developing digital economy, and to safeguard consumer trust, Congress needs to enact new comprehensive privacy legislation that accomplishes the goals stated above. This would help ensure that the United States does not slip behind in this important area as privacy continues to be a dominant issue in the twenty-first century and beyond.

and Electronic Documents Act, and the Asia-Pacific Economic Cooperation Privacy Framework all utilize accountability principles. *Id.*

[150] There are, of course, some exceptions.