ONLINE PRIVACY PROTECTION: PROTECTING PRIVACY, THE SOCIAL CONTRACT, AND THE RULE OF LAW IN THE VIRTUAL WORLD

Matthew Sundquist[*]

TABLE OF CONTENTS

INTRODUCTION

A host of laws and regulations engage with the legal,[1] technological,[2] and social[3] meanings[4] of privacy. In a country of more

---

[*] Matthew Sundquist is a graduate of Harvard College. He is the Privacy Manager at Inflection and a Student Fellow of the Harvard Law School Program on the Legal Profession. This paper represents the opinion of the author. It is not meant to represent the position or opinions of Inflection. For their thoughtful advice and suggestions, the author is grateful to Ali Sternburg, Allison Anoll, Beth Givens, Bob Gellman, Bruce Peabody, Christopher Wolf, Erik Jones, Jacqueline Vanacek, James Grimmelmann, Orin Kerr, and Samuel Bjork. For their support in writing this paper and friendship, the author is grateful to Brian and Matthew Monahan.

[1] Privacy is a multifaceted legal concept. For a discussion of privacy as a principle in law, see generally Brief *Amicus Curiae* of the Liberty Project in Support of Petitioner, Kyllo v. United States, 533 U.S. 27 (2000) (No. 99-8508) (describing the historical roots of the right to privacy); Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335 (exploring privacy as a legal concept, rather than a philosophical or moral concept). Samuel D. Warren and Louis D. Brandeis famously described the right to privacy as the "right of the individual to be let alone." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890).

than 300 million people[5] and plentiful law enforcement officers, there is likely to be abusive behavior. As a result, our society is flooded with claims about the definition, function, and value of privacy; with potential threats to privacy; and, increasingly, with debates about how to fashion remedies to address these issues. To survey the entire landscape of privacy dilemmas and threats, or to attempt to extract a representative sample of privacy policies and dilemmas, would be unwieldy and unproductive. This Article does not attempt to provide a systematic,

---

Privacy is often covered by statutory law, *see* statutes cited *infra* note 88, and the Supreme Court has repeatedly acknowledged privacy rights, *see, e.g.*, Lawrence v. Texas, 539 U.S. 558, 567 (2003); Moore v. City of E. Cleveland, 431 U.S. 494, 499 (1977); Kelley v. Johnson, 425 U.S. 238, 251 (1976) (Marshall, J., dissenting); Stanley v. Georgia, 394 U.S. 557, 564 (1969); Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring); Griswold v. Connecticut, 381 U.S. 479, 483 (1965); Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); *Ex parte* Jackson, 96 U.S. 727, 733 (1877); *see also* Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1065–73 (2006) (reciting the history of privacy in the Supreme Court's Fourth Amendment jurisprudence).

[2] Technology has created intriguing privacy problems. *See* Rakesh Agrawal & Ramakrishnan Srikant, *Privacy-Preserving Data Mining*, SIGMOD REC., June 2000, at 439, 439 (attempting to "develop accurate [data mining] models without access to precise information in individual data records"); Latanya Sweeney, *k-Anonymity: A Model for Protecting Privacy*, 10 INT'L J. OF UNCERTAINTY, FUZZINESS & KNOWLEDGE-BASED SYS. 557, 562 (2002) (explaining how to release data while maintaining privacy); Horst Feistel, *Cryptography and Computer Privacy*, SCI. AM., May 1973, at 15, 15, 23 (exploring enciphering and origin authentication as a means of protecting systems and personal databanks).

[3] Scholars have often advocated balanced frameworks for interpreting and protecting privacy. *See* JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 75–78 (1997) (arguing that privacy entails informational privacy, accessibility privacy, and expressive privacy); JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 7 (2008) (arguing that the younger generation of technology users, due to its frequent and early adoption of technology, has different conceptions of privacy than its parents or grandparents); ALAN F. WESTIN, PRIVACY AND FREEDOM 31 (1967) (arguing that privacy is comprised of "solitude, intimacy, anonymity, and reserve"); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202–03 (1998) (arguing for privacy in our physical space, choice, and flow of personal information); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, DÆDALUS, Fall 2011, at 32, 33 [hereinafter *Privacy Online*] (arguing that "entrenched norms" form our privacy expectations for the flow of information).

[4] I examine privacy of the personal information we create directly by communicating and completing forms, contracts, and documents as well as the information we create indirectly by using browsers, carrying phones with geo-tracking, and purchasing or using products and services. I focus on the assurances we receive about this information and whether they are complied with. *See* Memorandum from Clay Johnson III, Deputy Dir. for Mgmt., to the Heads of Exec. Dep'ts & Agencies 1–2 (May 22, 2007), *available at* http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf (defining "personally identifiable information" and recommending steps to protect that information).

[5] PAUL MACKUN & STEVEN WILSON, U.S. CENSUS BUREAU, POPULATION DISTRIBUTION AND CHANGE: 2000 TO 2010, at 2 (2011).

theoretical account of privacy and technology, nor does it outline a typology of circumstances in which privacy might be threatened or abused by private or public entities. Instead, this Article advances a general framework for identifying circumstances wherein a legal or social response to a privacy threat is appropriate. The emergent areas I survey demonstrate the utility and application of my approach.

This Article is divided into four Parts. Part I introduces the following framework for assessing whether a virtual or online practice, law, or regulatory deficiency warrants a legal or social response: (1) a practice that violates the law should be prosecuted; (2) privacy laws that are ineffectually enforced necessitate heightened alert; and (3) an effective response is needed when a practice violates a valued social expectation regarding how information should flow.[6] Updating and enforcing our laws in light of technological change is crucial to the maintenance of the social contract, making the first two aspects of this framework vital to protecting privacy. Many of our expectations about information and privacy developed when tracking at the scale the government and businesses do so now was impossible. Information often flows based on what is technologically possible rather than on what is socially or legally acceptable.[7] These new realities require a novel response, as mandated by my third condition.

Part II examines how technology has allowed more information about people to be gathered and stored online.[8] Technology has, as Amazon founder Jeff Bezos explained, begun "eliminating all the gatekeepers" for companies and technical practices.[9] Vast digital trails are created by the approximately ninety percent of online adults who report using email or an online search engine on an average day.[10] The National Security Agency can intercept and download electronic communications equivalent to the contents of the Library of Congress every six hours.[11] And further, when challenged, businesses and the

---

[6] *See Privacy Online*, *supra* note 3, at 45 ("If pursued conscientiously, the process of articulating context-based rules and [privacy] expectations and embedding some of them in law and other specialized codes will yield the safety nets that buttress consent in fields such as health care and research.").

[7] *Id.* at 34.

[8] *See* Sweeney, *supra* note 2, at 557 ("Society is experiencing exponential growth in the number and variety of data collections containing person-specific information as computer technology, network connectivity and disk storage space become increasingly affordable.").

[9] Thomas L. Friedman, *Do You Want the Good News First?*, N.Y. TIMES, May 20, 2012, § SR (Sunday Review), at 1.

[10] KRISTEN PURCELL, PEW RESEARCH CTR., SEARCH AND EMAIL STILL TOP THE LIST OF MOST POPULAR ONLINE ACTIVITIES 2 (2011), *available at* http://pewinternet.org/~/media//Files/Reports/2011/PIP_Search-and-Email.pdf.

[11] Jane Mayer, *The Secret Sharer: Is Thomas Drake an Enemy of the State?*, NEW

government can quickly create and begin to rely on new online practices they claim to be essential,[12] while in the process contributing to the growth of a massive online-tracking industry.[13]

While economic theory suggests people possess a rational capacity to process the stream of privacy threats and trade-offs we face, people simply cannot be expected to effectively navigate this uncertain terrain on their own.[14] Regulatory inaction—or a lack of regulations altogether—allows for more activity and the potential for further privacy violations to happen faster and at a larger scale.

Part III points out specific areas for change and argues for better laws, better case-precedents that weigh social expectations of privacy when determining what constitutes a reasonable expectation of privacy, and better enforcement efforts. Even as courts and Congress have addressed some questions involving the relationship between evolving technology and privacy, including constitutional issues, they have avoided others. The Supreme Court in recent years, for example, has declined to address whether the police can electronically track citizens[15] and has failed to examine whether texting on two-way pagers is private.[16] Additionally, Congress has not updated key privacy legislation[17] and has not responded when the government has invoked its

---

YORKER, May 23, 2011, at 47, 49 ("Even in an age in which computerized feats are commonplace, the N.S.A.'s capabilities are breathtaking. . . . Three times the size of the C.I.A., and with a third of the U.S.'s entire intelligence budget, the N.S.A. has a five-thousand-acre campus at Fort Meade protected by iris scanners and facial-recognition devices. The electric bill there is said to surpass seventy million dollars a year."). Additionally, government analysts annually produce 50,000 intelligence reports. Dana Priest & William M. Arkin, *A Hidden World, Growing Beyond Control*, WASH. POST, July 19, 2010, at A1.

[12] *See generally* Comments from Pam Dixon, Exec. Dir., World Privacy Forum, to the Fed. Trade Comm'n (Feb. 18, 2011), *available at* www.ftc.gov/os/comments/privacyreportframework/00369-57987.pdf (discussing the Federal Trade Commission's narrow focus on online tracking).

> The Commission needs to focus on the broader picture here and to try to get ahead of developments before they become so embedded in business practices that any limit will be fought as the *end of the world as we know it*, a cry heard too often on the Internet.

Id. at 6.

[13] *See* Anne Klinefelter, *When to Research Is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking*, 16 VA. J.L. & TECH. 1, 5–18 (2011) (discussing the growth of the online tracking industry).

[14] *See infra* Part II. S*ee generally* Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, IEEE SECURITY & PRIVACY, Jan.–Feb. 2005, at 26, 26–27.

[15] United States v. Jones, 132 S. Ct. 945, 950 (2012).

[16] City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010).

[17] *See* discussion *infra* Part III.B.

"secret interpretations" of the Patriot Act.[18] Regulatory agencies have accepted trivial concessions and non-financial settlements from companies charged with breaking the law.[19] Meanwhile, leaders struggle to grasp technology, and election-focused politicians prefer solving problems to preventing them as this yields greater credit from constituents.[20]

Lastly, Part IV concludes with a case study examining the recent Federal Trade Commission ("FTC") settlements with Google and Facebook. Both companies broke laws and violated our social expectations, settled with either undersized financial settlements or none at all, and then made trivial concessions to their customers and the FTC.[21] And while both companies continue to perpetrate similar offenses, the FTC rarely responds. The actions of these companies and the ensuing lack of enforcement meet all three criteria demanding a response: bad laws, broken social expectations, and deficient enforcement. I argue for better laws, better enforcement, and a change in the professional culture and values of the FTC. In conclusion, I draw lessons from the successful opposition to the Stop Online Piracy Act and emphasize the importance of privacy education.

I. VALUING PRIVACY AND DETERMINING WHEN TO RESPOND

Justice Brandeis considered privacy—"the right to be let alone"—to be "the most comprehensive of rights and the right most valued by civilized men."[22] But why is privacy so valuable and important?[23] Presumably, privacy has a political value in deterring government overreach into our lives. Privacy also seems necessary to ensure citizens can discuss and voice their views in private without fear of outside intervention, thus ensuring democratic participation.[24] It is, however,

---

[18] Letter from Ron Wyden & Mark Udall, U.S. Senators, to Eric Holder, U.S. Att'y Gen. (Mar. 15, 2012) (on file with Regent University Law Review).

[19] *See* discussion *infra* Part IV.

[20] *See* discussion *infra* Part III.C.

[21] *See* discussion *infra* Part IV.

[22] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[23] While I briefly examine this question, others have given the subject a thorough treatment. *See generally* Paul A. Freund, *Privacy: One Concept or Many*, *in* PRIVACY NOMOS XIII 182, 195–96 (J. Roland Pennock & John W. Chapman eds., 1971) (arguing that privacy "serves an important socializing function"); James Rachels, *Why Privacy Is Important*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 290, 290–99 (Ferdinand David Schoeman ed., 1984).

[24] Thomas B. Kearns, *Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns*, 7 WM. & MARY BILL RTS. J. 975, 978 (1999) ("Without the ability to interact with one another in private, individuals cannot exchange ideas freely. This 'marketplace of ideas' is essential for a democracy to function properly and give rise to a free society."); *see also* Valerie Steeves, *Privacy and New Media*,

difficult to categorize privacy as a value,[25] let alone to quantify its risks or benefits.[26] We value some things as instrumental goods, for example, which provide a means to an end, like money. We also value intrinsic moral goods and virtues, like justice.[27] Privacy, however, is difficult to categorize as either clearly intrinsic or clearly instrumental. Professor Charles Fried notes, "[W]e do not feel comfortable about asserting that privacy is intrinsically valuable, an end in itself—privacy is always for or in relation to something or someone. On the other hand, to view privacy as simply instrumental, as one way of getting other goods, seems unsatisfactory too."[28]

So what is the value of privacy? Privacy creates a framework that allows other values to exist and develop. Where privacy is available, we can have freedom, liberty, and other intrinsic goods. We can develop friendships, relationships, and love.[29] As anyone who has had a camera pointed at them knows, we act differently when being recorded. Now consider that everything we do online, over the phone, or with a credit card can be monitored and recorded. If this information is used abusively, similar to how we might feel if we were filmed all the time, it compromises our ability to act naturally and freely. A social dynamic exists in this as well. In society, when people are around, we must react to external stimulants and forces. But alone, we can choose and create our stimulants and environment and react accordingly. Thus, we develop as independent beings and people when we have privacy.[30]

At this point, it is also worth addressing two common arguments against privacy. The first says, "You needn't worry about privacy if you haven't done anything wrong." I ask people making this argument if they believe they are doing something wrong by showering. They usually say "no." I then ask if they would be comfortable having a video of their

---

in MEDIASCAPES: NEW PATTERNS IN CANADIAN COMMUNICATION 250, 255–57 (Paul Attallah & Leslie Regan Shade eds., 2d ed. 2006).

[25] For a thorough discussion of this problem, see Jeffery L. Johnson, *A Theory of the Nature and Value of Privacy*, 6 PUB. AFF. Q. 271, 272, 276–77 (1992).

[26] *See* Adam Shostack & Paul Syverson, *What Price Privacy? (and Why Identity Theft Is About Neither Identity nor Theft)*, *in* ECONOMICS OF INFORMATION SECURITY 129, 129, 133–35 (L. Jean Camp & Stephen Lewis eds., 2004).

[27] *See* Michael J. Zimmerman, *Intrinsic vs. Extrinsic Value*, STAN. ENCYCLOPEDIA PHIL. (Dec. 17, 2010), http://plato.stanford.edu/entries/value-intrinsic-extrinsic/.

[28] Charles Fried, *Privacy: A Rational Context*, *in* TODAY'S MORAL PROBLEMS 21, 21 (Richard Wasserstrom ed., 1975).

[29] *Id.* at 25 ("[P]rivacy creates the moral capital which we spend in friendship and love.").

[30] *See* Robert F. Murphy, *Social Distance and the Veil*, 66 AM. ANTHROPOLOGIST 1257, 1259 (1964) ("Interaction is threatening by definition, and reserve, here seen as an aspect of distance, serves to provide partial and temporary protection to the self. . . . [T]he privacy obtained makes other roles more viable . . . .").

shower projected to the internet. Again, the answer is usually "no." The point is this: we do, write, and say things, as individuals and in relationships, that, while not wrong, are private. We are comfortable showering, expressing our vulnerabilities or beliefs, or confessing our love because we believe our actions are private. Violating that security undermines our person, actions, and relationships. A second common argument is that we should trust the government to guard us against terrorism, crime, etc. As I discuss throughout this Article, the government and corporations often act in secret, shrouded behind a veil of secrecy that has permitted abuse of our privacy and existing laws. Secrecy, law-breaking, and privacy abuses, in my view, suggest we should closely scrutinize privacy practices and those managing them.

Given the value of privacy, I posit we should prioritize privacy threats of three types: (1) law-breaking; (2) insufficient enforcement; and (3) subversion of social expectations by laws, practices, or frameworks. The first two speak to the role of government and the social contract. According to the social contract, a pervasive idea in American society and government,[31] we trade the state of nature—the world without government—to form a society and enjoy protection, security, and property.[32] To protect our values, we create laws tasked with the goal of "secur[ing] a situation whereby moral goals which, given the current social situation in the country whose law it is, would be unlikely to be achieved without it."[33] The law should serve the common interest and secure values that will be broadly useful to society.[34] Once established, the law (and associated rules) must be enforced[35] since the government

---

[31] Anita L. Allen, *Social Contract Theory in American Case Law*, 51 FLA. L. REV. 1, 3 (1999) ("According to some historians, the American colonists relied upon liberal, Lockean notions of a social contract to spirit rebellion against unwanted British rule. Historians have maintained that social contractarian theories of political order significantly influenced the people who wrote and defended the Declaration of Independence, the original Constitution, and the Bill of Rights."); Christine N. Cimini, *The New Contract: Welfare Reform, Devolution, and Due Process*, 61 MD. L. REV. 246, 275 (2002) ("[T]he Declaration of Independence, original state constitutions, the Articles of Confederation, and the federal Constitution with its accompanying Bill of Rights all based their notions of the structure of democratic government on ideas of social contract. These documents amount to a formalization of the social contract between the government and its people.").

[32] *See* JOHN LOCKE, THE SECOND TREATISE OF GOVERNMENT 48–50 (Thomas P. Peardon ed., The Bobbs-Merrill Co. 1952) (1690); JEAN JACQUES ROUSSEAU, THE SOCIAL CONTRACT 12–15 (Willmoore Kendall trans., Henry Regnery Co. 1954) (1762).

[33] Joseph Raz, *About Morality and the Nature of Law*, 48 AM. J. JURIS. 1, 12 (2003) [hereinafter *About Morality*].

[34] *See* JOHN RAWLS, A THEORY OF JUSTICE 29, 83, 187 (rev. ed. 1999).

[35] *See, e.g.*, Joseph Raz, *Reasoning With Rules*, 54 CURRENT LEGAL PROBS. 1, 18 (2001) ("Again we can see how rules are the inevitable backbone of any structure of authority, of which the law is a paradigm example.").

derives authority from creating and enforcing laws.[36] Thus, there is an immediate, positive benefit when we protect a valued good like privacy. Additionally, there is a broader benefit, as enforcing the law gives the government credibility and creates a stable society.[37]

The third prong of my privacy framework values social expectations. Norms and expectations allow people to feel secure and ensure that society functions well.[38] Privacy is a social expectation based on the ways in which information is collected and gathered. As Dr. Helen Nissenbaum points out, "When the flow of information adheres to entrenched norms, all is well; violations of these norms, however, often result in protest and complaint."[39] Problematically, technological limitations change and disappear quickly, allowing information to flow without the guidance of current expectations or social, ethical, legal, and political norms.[40] Businesses should nonetheless act in accordance with our social expectations, and when they do not, courts and legislatures should step in to protect those expectations. As noted, privacy has a value for us, and unmet expectations of privacy enforcement undermine our ability to be secure in our person and development. Exploitations and privacy invasions will persist if we do not respond, but as I detail in the next Part, regulating technology trends is costly, complicated, and cumbersome.

---

[36] *See About Morality*, *supra* note 33, at 7–9.

[37] *See* RAWLS, *supra* note 34, at 154–55. Indeed, people expect good laws and efficient governmental enforcement; in one survey, ninety-four percent of internet users said that privacy violators should be disciplined. SUSANNAH FOX, PEW RESEARCH CTR., TRUST AND PRIVACY ONLINE: WHY AMERICANS WANT TO REWRITE THE RULES 3 (2000), *available at* http://www.pewinternet.org/~/media//Files/Reports/2000/PIP_Trust_Privacy_Report.pdf.pdf. Social contract theory is primarily based on natural law. Nonetheless, the legislative and judicial support for privacy, as well as the social expectation of the legal enforcement of privacy in the U.S., evidenced in part by the Pew Research Center findings, demonstrate that natural law arguments and legal positivism can be invoked to support the framework. However, I do not engage substantially with legal positivism in this paper, as I believe others have done so much more thoughtfully than I could. *See generally* RONALD DWORKIN, LAW'S EMPIRE (1986) (emphasizing the interpretive defects of positivism); RONALD DWORKIN, TAKING RIGHTS SERIOUSLY (1978) (defending a liberal theory of law and arguing against legal positivism and the theory of utilitarianism); Leslie Green, *Legal Positivism*, STAN. ENCYCLOPEDIA PHIL. (Jan. 3, 2003), http://plato.stanford.edu/entries/legal-positivism/ ("What laws are in force in that system depends on what social standards its officials recognize as authoritative; for example, legislative enactments, judicial decisions, or social customs.").

[38] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 3, 128 (2010).

[39] *Privacy Online*, *supra* note 3, at 33.

[40] *See id.* at 34.

II. COMPOUNDING PRIVACY PROBLEMS: RATIONAL CHOICE THEORY AND TECHNOLOGICAL GROWTH

Each year, consumers share more and more information online as a result of increased participation in internet activities.[41] Today, nearly half of American adults use smartphones.[42] In 2014, mobile data usage is projected to be at 3,506% of what it was in 2009.[43] Furthermore, "[t]he number of worldwide email accounts is expected to increase from . . . 3.1 billion in 2011 to nearly 4.1 billion by year-end 2015."[44]

By exploiting this technological growth, businesses and the government are capable of using private information in ways that would have been impossible just a few years ago. As such, our expectations are outdated. Consider, for example, that Lotame Solutions uses web beacons that record what a person types on a website in order to create a user profile,[45] while Apple,[46] Verizon,[47] Target,[48] and others[49] compile

---

[41] *See, e.g.*, PURCELL, *supra* note 10, at 3 ("In January 2002, 52% of *all Americans* used search engines and that number grew to 72% in [2011]. In January 2002, 55% of *all Americans* said they used email and that number grew to 70% in [2011]."); U.S. CENSUS BUREAU, E-STATS 1 (2010), *available at* http://www.census.gov/econ/estats/2010/2010reportfinal.pdf (reporting that, in 2010, e-commerce grew faster than total economic activity, retail e-commerce sales increased 16.3% from 2009 to 2010, and e-commerce in the manufacturing industry accounted for 46.4% of total shipments for 2010).

[42] AARON SMITH, PEW RESEARCH CTR., 46% OF AMERICAN ADULTS ARE SMARTPHONE OWNERS 2 (2012), *available at* http://pewinternet.org/~/media//Files/Reports/2012/Smartphone%20ownership%202012.pdf.

[43] FED. COMMC'NS COMM'N, MOBILE BROADBAND: THE BENEFITS OF ADDITIONAL SPECTRUM, FCC STAFF TECHNICAL PAPER 18 (2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-302324A1.pdf.

[44] THE RADICATI GRP., INC., EMAIL STATISTICS REPORT, 2011–2015—EXECUTIVE SUMMARY 2–3 (2011), *available at* http://www.radicati.com/wp/wp-content/uploads/2011/05/Email-Statistics-Report-2011-2015-Executive-Summary.pdf.

[45] Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 31–Aug. 1, 2010, at W1.

[46] Nick Bilton, *Tracking File Found in iPhones*, N.Y. TIMES, Apr. 21, 2011, at B1 ("[A] new hidden file [on iPhones and certain iPads] began periodically storing location data, apparently gleaned from nearby cellphone towers and Wi-Fi networks, along with the time. The data is stored on a person's phone or iPad, but when the device is synced to a computer, the file is copied over to the hard drive . . . .").

[47] David Goldman, *Your Phone Company Is Selling Your Personal Data*, CNNMONEY (Nov. 1, 2011, 10:14 AM), http://money.cnn.com/2011/11/01/technology/verizon_att_sprint_tmobile_privacy/index.htm ("In mid-October, Verizon Wireless changed its privacy policy to allow the company to record customers' location data and Web browsing history, combine it with other personal information like age and gender, aggregate it with millions of other customers' data, and sell it on an anonymous basis.").

[48] Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, Feb. 19, 2012, § 6 (Magazine), at 30 ("[L]inked to your [Target] Guest ID is demographic information like your age, whether you are married and have kids, which part of town you live in, how long it takes you to drive to the store, your estimated salary, whether you've moved recently, what credit cards you carry in your wallet and what Web sites you visit.").

information from customers' interactions with their products. Roughly 1,271 government organizations and 1,931 private companies work on "counterterrorism, homeland security and intelligence in about 10,000 locations across the United States."[50] It is estimated that 854,000 people hold top-secret security clearances.[51] Using a GPS device, police can do what would have formerly required "a large team of agents, multiple vehicles, and perhaps aerial assistance."[52] As a result, technology untested by law has flourished—examples include respawning cookies,[53] beacons and flash cookies,[54] and browser-history sniffing.[55] Governments and businesses build around new, unregulated technology and practices and then claim that changes would endanger their business or national security.[56]

Moreover, although mainstream microeconomic theory suggests we have a rational capacity to process information about privacy tradeoffs to which we assent in online activities, the fact of the matter is that choices about terms-of-use, browser settings and software, and purchases and credit cards, etc., are complicated, making it unlikely that the "complete information" criterion of rationality will be met when we face privacy decisions.[57] Even with full information, we may act against our better

---

[49] Natasha Singer, *Following the Breadcrumbs on the Data-Sharing Trail*, N.Y. TIMES, Apr. 29, 2012, § BU (Sunday Business), at 4 ("In the United States, with the exception of specific sectors like credit and health care, companies are free to use their customers' data as they deem appropriate. That means every time a person buys a car or a house, takes a trip or stays in a hotel, signs up for a catalog or shops online or in a mall, his or her name might end up on a list shared with other marketers.").

[50] Priest & Arkin, *supra* note 11.

[51] *Id.*

[52] United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring).

[53] "Respawning" is "the ability to reinstate standard cookies that are deleted or otherwise lost by the user." Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 278 (2012).

[54] *Tracking the Trackers: Our Method*, WALL ST. J., July 31–Aug. 1, 2010, at W3 ("HTML cookies are small text files, installed on a user's computer by a website, that assign the user's computer a unique identity and can track the user's movements on a site. . . . Beacons are bits of software code on a site that can transmit data about a user's browsing behavior.").

[55] Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281, 299–300 (2012) ("Browser history sniffing exploits the functionality of browsers that display hyperlinks of visited and non-visited sites in different colors . . . . Websites apparently exploited this functionality by running Javascript code in order to list hundreds of URLs, thereby recreating a user's browsing history—all without the user's knowledge or consent.").

[56] *See* Dixon, *supra* note 12, at 6.

[57] *See* Acquisti & Grossklags, *supra* note 14, at 26–27. *See generally* 3 HERBERT A. SIMON, MODELS OF BOUNDED RATIONALITY: EMPIRICALLY GROUNDED ECONOMIC REASON 291–94 (1997). It is worth noting that there are similar rational bounds to our capacity to understand medicine, science, finance, etc.

judgment, owing to lack of self-control, false belief that we are immune from harm, or a desire for immediate gratification.[58] Privacy decision-making and privacy features are also incredibly complex.[59] Users cannot research these settings under reasonable circumstances, much less choose between them.[60] In a recent study of forty-five experienced web-users, participants were instructed to activate browsers and tools to block cookies.[61] Users blocked much less than they thought they did, often blocking nothing.[62] Users were unable to apply tools designed for privacy, while companies and governments creating technological, legal, and societal defaults aim to gather information.[63] Behavioral economics offers insight into these problems.[64] As I address in the next Part, comprehension challenges are compounded by legal confusion, inaction, and non-compliance.

III. LEGAL AND JUDICIAL PRIVACY GUIDANCE

A. Precedents

Chief Justice John Marshall said that it is "emphatically the province and duty of the judicial department to say what the law is."[65] The Supreme Court should do so in a manner that corresponds to social expectations regarding privacy in the virtual world we live in today. The Supreme Court has recognized that new technology can "shrink the realm of guaranteed privacy,"[66] and it should consider new technology as a highly relevant factor when defining "the existence, and extent, of privacy expectations" under our Fourth Amendment privacy

---

[58] Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*, *in* EC'04: PROCEEDINGS OF THE 5TH ACM CONFERENCE ON ELECTRONIC COMMERCE 21, 24 (2004).

[59] An examination of 133 privacy-software tools and services revealed a list of 1,241 privacy-related features. Benjamin Brunk, *Understanding the Privacy Space*, FIRST MONDAY (Oct. 7, 2002), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/991/912.

[60] *See id.*

[61] PEDRO G. LEON ET AL., WHY JOHNNY CAN'T OPT OUT: A USABILITY EVALUATION OF TOOLS TO LIMIT ONLINE BEHAVIORAL ADVERTISING 8–9 (2012), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf.

[62] *Id.* at 15.

[63] *Id.* at 14; *see also* MICHELLE MADEJSKI ET AL., THE FAILURE OF ONLINE SOCIAL NETWORK PRIVACY SETTINGS 1 (2011), *available at* http://www.cs.columbia.edu/~maritzaj/publications/2011-tr-madejski-violations.pdf ("We present the results of an empirical evaluation that measures privacy attitudes and intentions and compares these against the privacy settings on Facebook. Our results indicate a serious mismatch: every one of the 65 participants in our study confirmed that at least one of the identified violations was in fact a sharing violation.").

[64] *See, e.g.*, Acquisti, *supra* note 58, at 21–22, 27.

[65] Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803).

[66] Kyllo v. United States, 533 U.S. 27, 34 (2001).

guaranties.[67] Nonetheless, the Court has been cautious when grafting privacy protections and expectations onto technological changes: the Justices waited nearly a century after the invention of the telephone to protect phone calls from unwarranted government surveillance and, even then, granted protections only when the individual was justified in relying on the privacy of the conversation.[68] The Court now applies a two-part test, developed in Justice Harlan's concurrence in *Katz v. United States*, to determine whether an individual's Fourth Amendment rights are invoked. In order for government activity to fall under the gambit of the Fourth Amendment, (1) the activity must encroach on "an actual (subjective) expectation of privacy," and (2) "the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[69]

We do expect that certain technology will not be used to exploit, expose, or abuse our privacy.[70] Federal courts have occasionally protected these expectations as they relate to government activity,[71] but

---

[67] City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010); *see also* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

[68] Katz v. United States, 389 U.S. 347, 352–53 (1967). For more instances of courts attempting to reconcile the Fourth Amendment with advances in technology, see United States v. Jones, 132 S. Ct. 945, 949–50 (2012) (holding that a vehicle is an "effect" as that term is used in the Fourth Amendment and that the warrantless use of a GPS tracking device constituted a search that violated the Fourth Amendment); United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1004–06 (9th Cir. 2009) (holding that the difficulty of separating electronic data that can be seized under a valid warrant from that which is not must not be allowed to become a license for the government to access broad, vast amounts of data which it has no probable cause to access).

[69] *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *see* Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (explaining that the established *Katz* test "has come to mean the test enunciated by Justice Harlan's separate concurrence in *Katz*"); Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 427 (2007) ("In subsequent cases, the Court has adopted Justice Harlan's two-pronged formulation of Fourth Amendment application as the standard analysis for determining whether or not a search has occurred.").

[70] In one survey, ninety-one percent of respondents were concerned their identities might be stolen and "used to make unauthorized purchases." *Zogby Poll: Most Americans Worry About Identity Theft*, IBOPE INTELIGÊNCIA (Apr. 3, 2007), http://www.ibopezogby.com/news/2007/04/03/zogby-poll-most-americans-worry-about-identity-theft/. Ninety percent of cloud-computing users in the United States "would be very concerned" if cloud service providers sold their files to a third party. JOHN B. HORRIGAN, PEW RESEARCH CTR., USE OF CLOUD COMPUTING APPLICATIONS AND SERVICES 2, 7 (2008), *available at* http://www.pewinternet.org/~/media/Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf.

[71] *See, e.g.*, *Kyllo*, 533 U.S. at 29–30, 34, 40 (holding that warrantless use of a thermal imaging device to detect heat emanating from a home constitutes an unlawful search and stating that to hold otherwise "would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment"); United States v. Warshak, 631 F.3d 266,

the Supreme Court has been hesitant to address the Fourth Amendment's relationship to recent technology, particularly in two cases. First, in *United States v. Jones*, the Court concluded that police must have a warrant to *place* a GPS tracker on a car because doing so and then using the device to monitor an individual is a Fourth Amendment search.[72] To be sure, this decision aligns with current societal expectations: a recent poll reveals that seventy-three percent of Americans believe police must have a warrant to put a GPS tracking device on a car.[73] Some members of the Court even recognized that long-term GPS monitoring without a warrant violates our social expectations.[74] The Court thought that tracking someone electronically (as opposed to placing the GPS on the vehicle) *could* be "an unconstitutional invasion of privacy."[75] The Court, however, concluded that addressing that question would lead "needlessly into additional thorny problems,"[76] despite our social expectations and the reality that long-term GPS monitoring is decreasingly reliant on an actual GPS device.[77] Second, in *City of Ontario v. Quon*, a case involving messages on a two-way pager, the Court faced what Justice Kennedy termed "issues of farreaching significance."[78] In its opinion, however, the Court avoided such issues, deeming two-way pagers, a decades-old device, an "emerging technology."[79] The judiciary, Kennedy concluded, would take a risk by engaging "the Fourth Amendment implications of emerging technology before its role in society has become clear."[80] At least one court sees this decision as unhelpful.[81]

Hesitancy and delay in recognizing social expectations is an inevitable outcome of the relationships among case law, technology, and legislation. Cases do not rise to the courts until years after an incident has occurred, and courts are beholden to the laws of Congress.

---

288 (6th Cir. 2010) (holding that the government may not force a commercial internet service provider to provide it with the contents of subscribers' emails).

72 *Jones*, 132 S. Ct. at 949.

73 FAIRLEIGH DICKINSON UNIV.'S PUBLICMIND POLL, HIGH COURT AGREES WITH PUBLIC IN US V. JONES: ELECTRONIC TAILS NEED A WARRANT 1 (2012), *available at* http://publicmind.fdu.edu/2012/tailing/final.pdf.

74 *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

75 *Id.* at 954.

76 *Id.*

77 *See id.* at 963–64 (Alito, J., concurring).

78 City of Ontario v. Quon, 130 S. Ct. 2619, 2624 (2010).

79 *Id.* at 2629.

80 *Id.*

81 *See* Rehberg v. Paulk, 611 F.3d 828, 844 (11th Cir. 2010) ("The Supreme Court's more-recent precedent [in *Quon*] shows a marked lack of clarity in what privacy expectations as to content of electronic communications are reasonable.").

Nonetheless, by the time a case reaches the Supreme Court, social expectations may be settled.[82] The Court should recognize this reality and find that certain communications and movement carry reasonable privacy expectations that society is prepared to recognize.

Justice Brennan believed that "[j]udges cannot avoid a definitive interpretation because they feel unable to, or would prefer not to, penetrate to the full meaning of the Constitution's provisions."[83] Judges can apply Fourth Amendment rules to the virtual world without creating new jurisprudence or frameworks.[84] Just as information in briefcases carries privacy protections,[85] so also our virtual identities, full of photos, correspondences, address books, etc., should carry similar protections.[86] The Court need not create a new privacy doctrine or theorize in a black box about expectations, as it can rely on polling to examine the social-expectation part of the *Katz* test. Polling is becoming increasingly easy to conduct and to evaluate for accuracy.[87] By using polling, the Court can determine and validate our social privacy expectations.

B. Statutory Guidance

A host of legislation addresses privacy.[88] No office or piece of legislation covers all personal information, however.[89] I apply my

---

[82] For example, seventy-three percent of participants in a recent poll viewed it as extremely important not to have someone watching or listening to them without permission. HUMPHREY TAYLOR, HARRIS INTERACTIVE, MOST PEOPLE ARE "PRIVACY PRAGMATISTS" WHO, WHILE CONCERNED ABOUT PRIVACY, WILL SOMETIMES TRADE IT OFF FOR OTHER BENEFITS 2 (2003), *available at* http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf.

[83] William J. Brennan, Jr., Speech to Georgetown University's Text and Teaching Symposium (Oct. 12, 1985), *in* THE GREAT DEBATE: INTERPRETING OUR WRITTEN CONSTITUTION 11, 13 (1986).

[84] *See, e.g.*, Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1048–49 (2010).

[85] United States v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983).

[86] *See* New Jersey v. T.L.O., 469 U.S. 325, 339 (1985) (noting that students who carry school supplies, keys, money, hygiene supplies, purses, wallets, photographs, letters, and diaries to school do so without "necessarily waiv[ing] all rights to privacy in such items merely by bringing them onto school grounds"); David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2219–20 (2009).

[87] *See* Nate Silver, *The Uncanny Accuracy of Polling Averages*, Part II: What the Numbers Say*, N.Y. TIMES (Sept. 30, 2010, 6:54 PM), http://fivethirtyeight.blogs.nytimes.com/2010/09/30/the-uncanny-accuracy-of-polling-averages-part-2-what-the-numbers-say/.

[88] *See, e.g.*, Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3402–3403(a) (2006); Fair Credit Reporting Act, 15 U.S.C. § 1681c(a) (2006); Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. § 1681m(e) (2006); Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6502 (2006); Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2006); Sarbanes-Oxley Act of 2002, 15 U.S.C. § 7215(b)(5)(A) (2006); Stored

framework to three laws, pinpointing areas where legislation or a lack of legislation allows abuse, subversion, or violations of social expectations of privacy. Outdated legislation can become problematic in application, as can legislation with overly broad coverage of technology, people, and content. It is crucial to examine how federal agencies gather, use, and disclose our information and, because of the inherent impact on the social contract, whether the government keeps its word and mandates compliance with the law.

The Privacy Act of 1974 ("Privacy Act") regulates how the government may gather, use, and distribute personal information.[90] It states, "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains . . . ."[91] But the Privacy Act only applies to the public sector. Members of Congress can skirt it by releasing information gathered by the government and buying back repurposed, enhanced versions of that information from data brokers.[92] Moreover, a Congressional Research Service report found that twenty-three federal agencies disclosed the personal information of their websites' users to other agencies, and at least four agencies shared the information with banks, retailers, distributors, and trade organizations.[93] The Privacy Act has about a

---

Communications Act, 18 U.S.C. § 2701(a) (2006); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b)(1) (2006); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721(a) (2006); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g(a)(2) (2006); Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320a-7c(a)(3)(B)(ii) (2006); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2006). This non-exhaustive list does not include state laws.

89 Julia Angwin, *Watchdog Planned for Online Privacy*, WALL ST. J. (Nov. 11, 2010, 8:03 PM), http://online.wsj.com/article/SB10001424052748703848204575608970171176014.html ("There is no comprehensive U.S. law that protects consumer privacy online."); *see also* ORG. FOR ECON. CO-OPERATION & DEV., INVENTORY OF INSTRUMENTS AND MECHANISMS CONTRIBUTING TO THE IMPLEMENTATION AND ENFORCEMENT OF THE OECD PRIVACY GUIDELINES ON GLOBAL NETWORKS 47–48 (1999) (showing the patchwork of legislation making up United States personal-information privacy law).

90 Privacy Act of 1974, 5 U.S.C. § 552a(a)–(e) (2006).

91 *Id.* § 552a(b).

92 Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1138–39 (2002) ("[T]he government routinely pour[s] [personal] information into the public domain . . . by posting it on the Internet . . . . This expanded profile would then be sold back to the government . . . ."). *See generally* Melissa Carrie Oppenheim, *The Dark Data Cycle: How the U.S. Government Has Gone Rogue in Trading Personal Data from an Unsuspecting Public* (Mar. 2012) (unpublished thesis, Harvard University) (thesis on file with the Regent University Law Review).

93 HAROLD C. RELYEA, CONG. RESEARCH SERV., RL 30824, THE PRIVACY ACT: EMERGING ISSUES AND RELATED LEGISLATION 5 (2002).

dozen exceptions,[94] including a widely-criticized,[95] broad exemption for "routine use."[96] There is little wonder it has been called "toothless."[97]

The Electronic Communications Privacy Act of 1986[98] ("ECPA") was drafted to protect the communication privacy of American citizens.[99] Written when copying records was a physical activity and records could be physically destroyed, the ECPA has not been significantly updated since it was passed in 1986. Applying it to email, texting, social networks, data storage, and other new technology is quite difficult.[100] Unnecessarily complex and overly technical distinctions—for instance, between opened and unopened email and email in transit and in storage—have emerged.[101] Although the ECPA may have seemed useful when it was passed, distinguishing privacy in this way or in other ways recognized by the ECPA now defies technological realities.

Lastly, the USA PATRIOT Act ("Patriot Act") defines the scope and types of information the federal government can gather in counter-terrorism efforts.[102] The Patriot Act allows the FBI to issue National Security Letters ("NSLs") with a demand for information and a gag order to prevent its recipient from discussing the request with anyone except an attorney (for legal advice) or someone "to whom such disclosure is

---

[94] § 552a(b)(1)–(12); *see also* PHILIPPA STRUM, PRIVACY: THE DEBATE IN THE UNITED STATES SINCE 1945, at 50 (1998).

[95] Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 584–85 (1995).

[96] § 552a(b)(3).

[97] ANNE S. KIMBOL, THE PRIVACY ACT MAY BE TOOTHLESS (2008), *available at* http://www.law.uh.edu/healthlaw/perspectives/2008/(AK)%20privacy%20act.pdf.

[98] Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2521 (2006).

[99] *See* S. REP. NO. 99-541, at 3, 5 (1986) ("With the advent of computerized recordkeeping systems Americans have lost the ability to lock away a great deal of personal and business information. . . . [T]he law must advance with the technology to ensure the continued vitality of the fourth amendment [sic]. . . . Congress must act to protect the privacy of our citizens. . . . The Committee believes that [the ECPA] represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies.").

[100] *See* Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. REV. 1043, 1045, 1073 (2008) (arguing that technology has outpaced the ECPA); *see also* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV 1375, 1396–97 (2004) ("Stored communications have evolved in such a way that [the ECPA's layers of statutory protection for stored communications] are becoming increasingly outdated and difficult to apply.").

[101] ROBERT GELLMAN, WORLD PRIVACY FORUM, PRIVACY IN THE CLOUDS: RISKS TO PRIVACY AND CONFIDENTIALITY FROM CLOUD COMPUTING 13 (2009) ("Distinctions recognized by ECPA include electronic mail in transit; electronic mail in storage for less than or more than 180 days; electronic mail in draft; opened vs. unopened electronic mail; electronic communication service; and remote computing service.").

[102] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 18 U.S.C. § 2516(1) (2006).

necessary to comply with the request."[103] From 2003 to 2006 the FBI issued nearly 200,000 NSLs,[104] which must certify a relevance of this information to "an authorized investigation to protect against international terrorism or clandestine intelligence activities."[105] Notwithstanding the remarkably broad nature of these guidelines, an internal FBI audit of ten percent of NSLs suggests that the FBI has violated these limitations more than 1,000 times.[106] While courts have intermittently regulated NSLs,[107] two senators familiar with the Patriot Act claim that

> there is now a significant gap between what most Americans think the law allows and what the government secretly claims the law allows. This is a problem, because it is impossible to have an informed public debate about what the law should say when the public doesn't know what its government thinks the law says.[108]

The obvious conclusion is that the best way to prevent secret invasions of our privacy is to ban secret invasions of our privacy. That solution, admittedly, is complex, and I address it in the following Sections.

C. Analysis

Voters' interests tend to be limited to very few issues in elections.[109] Congress has on a few occasions considered privacy legislation,[110] but privacy is generally a low political priority. Part of this is due to how Congress approaches oversight.[111] One model Congress could choose to

---

[103] *Id.* § 2709(c).

[104] *National Security Letters Reform Act of 2007: Hearing on H.R. 3189 Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 110th Cong. 11 (2008) (statement of Glenn A. Fine, Inspector General of the United States).

[105] § 2709(b)(1).

[106] John Solomon, *FBI Finds It Frequently Overstepped in Collecting Data*, WASH. POST, June 14, 2007, at A1; *see also* U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006, at 81 (2008) (noting that the Inspection Division of the FBI "identified 640 NSL-related possible intelligence violations in 634 NSLs").

[107] *E.g.*, John Doe, Inc. v. Mukasey, 549 F.3d 861, 883 (2d Cir. 2008).

[108] Wyden & Udall, *supra* note 18 (emphasis omitted).

[109] *See* Edward G. Carmines & James A. Stimson, *On the Structure and Sequence of Issue Evolution*, 80 AM. POL. SCI. REV. 901, 915 (1986) ("The issue space—that tiny number of policy debates that can claim substantial attention both at the center of government and among the passive electorate—is strikingly limited by mass inattention.").

[110] *See, e.g.*, Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. (2011); Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011); Building Effective Strategies to Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act, H.R. 611, 112th Cong. (2011).

[111] James B. Pearson, *Oversight: A Vital Yet Neglected Congressional Function*, 23 U. KAN. L. REV. 277, 281 (1975) ("Paradoxically, despite its importance, congressional oversight remains basically weak and ineffective."). *But see* Mathew D. McCubbins &

follow is the "police-patrol" model, which is "centralized, active, and direct."[112] Congress would pro-actively search for and remedy violations of its legislative goals.[113] Congress, however, seems to prefer a "fire-alarm" model that forces citizens and advocacy groups to bear the costs of detection.[114] Under this model, Congress establishes rules, procedures, and practices, but it requires individuals and interest groups to examine administrative decisions, charge those agencies that violate legislative goals, and seek remedies to hold those executive agencies accountable for their violations.[115] Legislators can then solve the problems, taking credit from those who sounded the alarm.[116] As noted, privacy is difficult to value and hard to understand, which may partially explain why Congress has not prioritized the issue.

Hyper-partisanship can impede compromise and action in the legislative branch,[117] and congressional members' interests in re-election can discourage active involvement in improving privacy policy.[118] Political parties also have the potential to shape our laws, but instead of championing privacy, both parties remain focused on using political processes to vie for power.[119] Established businesses have connections, experience, money, and lobbying capacity, and the government has far-reaching power. Privacy as a good, however, lacks these advantages. Under the shadow of discussions involving issues such as national security, child pornography, and the "War on Terror," privacy rights weaken. And, as previously mentioned, psychological processing

---

Thomas Schwartz, *Congressional Oversight Overlooked: Police Patrol Versus Fire Alarms*, 28 AM. J. POL. SCI. 165, 176 (1984) ("The widespread perception that Congress has neglected its oversight responsibility is a widespread mistake.").

[112] McCubbins & Schwartz, *supra* note 111, at 166.

[113] *Id.*

[114] *Id.* at 168.

[115] *Id.* at 166.

[116] *Id.* at 168.

[117] Sarah A. Binder, *The Dynamics of Legislative Gridlock, 1947–96*, 93 AM. POL. SCI. REV. 519, 527 (1999).

[118] *See* Gary Biglaiser & Claudio Mezzetti, *Politicians' Decision Making with Re-Election Concerns*, 66 J. PUB. ECON. 425, 442 (1997) (describing the "negative welfare effect" of politicians' re-election concerns). *See generally* DAVID R. MAYHEW, CONGRESS: THE ELECTORAL CONNECTION (2d ed. 2004).

[119] *See* Daryl J. Levinson & Richard H. Pildes, *Separation of Parties, Not Powers*, 119 HARV. L. REV. 2311, 2313 (2006) ("Political competition and cooperation along relatively stable lines of policy and ideological disagreement quickly came to be channeled not through the branches of government, but rather through an institution the Framers could imagine only dimly but nevertheless despised: political parties."); *see also* Ezra Klein, *The Unpersuaded*, NEW YORKER, Mar. 19, 2012, at 32, 38 ("[W]e have a system that was designed to encourage division between the branches but to resist the formation of political parties. The parties formed anyway, and they now use the branches to compete with one another.").

problems and the low salience of privacy as an issue to voters also seems to play a role in its failure to motivate significant public outcry. Yet if each branch of government accepts legislative and regulatory inaction to privacy abuse, the separation of powers[120] will likewise fail to protect privacy.[121]

D. Looking Ahead

Senators, scholars, and advocates have asserted that agencies are infringing on our privacy.[122] The Supreme Court cannot easily interpret poorly written or imprecise laws; it is much more difficult to serve as a supplemental lawmaker capable of applying congressional intent when congressional intent is unclear.[123] Congress must handle this type of large-scale public problem legislatively.[124] It should begin by holding public hearings to examine secret abuses and current privacy legislation to bring the issue into the public eye. Congress should then update obsolete frameworks in the ECPA and the Privacy Act, amending them with an eye toward current and future technology-use.[125] It should empower courts and administrative agencies to revisit these issues. As necessary, it should redefine and amend legislative goals,[126] particularly in areas of abused or subverted legislation. Where the Department of

---

[120] The Founders gave "each department, the necessary constitutional means, and personal motives, to resist encroachments of the others." THE FEDERALIST NO. 51, at 268 (James Madison) (George W. Carey & James McClellan eds., 2001); *see* John A. Fairlie, *The Separation of Powers*, 21 MICH. L. REV. 393, 393 (1923) ("This tripartite system of governmental authorities was the result of a combination of historical experience and a political theory generally accepted in this country as a fundamental maxim in the latter part of the eighteenth century.").

[121] *See generally* Bruce G. Peabody & John D. Nugent, *Toward a Unifying Theory of the Separation of Powers*, 53 AM. U. L. REV. 1, 44 (2003) (explaining the balance of powers and that the repetitive and staggered nature of United States policy creation can lead to a broad consensus and a guarantee that "contentious issues can be easily revisited"). Complacency among the branches can lead to inaction on other issues as well. *See, e.g.*, Matthew L. Sundquist, Worcester v. Georgia*: A Breakdown in the Separation of Powers*, 35 AM. INDIAN L. REV. 239, 255 (2010–2011).

[122] *See, e.g.*, *Privacy Online*, *supra* note 3, at 33, 41; Wyden & Udall, *supra* note 18.

[123] Beth M. Henschen, *Judicial Use of Legislative History and Intent in Statutory Interpretation*, 10 LEGIS. STUD. Q. 353, 353 (1985) ("Thus the role that the Supreme Court adopts as supplemental lawmaker depends in part on the opportunities for judicial policy making that Congress provides in its statutes.").

[124] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805–06 (2004).

[125] *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209 (2004) (recommending ways for Congress to amend the Stored Communications Act to better protect internet users' privacy).

[126] McCubbins & Schwartz, *supra* note 111, at 174 ("Congress also can redefine or reaffirm its goals by redefining or explicating the jurisdictional authority of an administrative agency.").

Justice has found violations within FBI and executive practices, it should vigilantly expose and oppose such violations. To counteract the fact that political leaders have trouble understanding technology,[127] Congress could rely on technologists when creating legislation, and courts could call on experts as witnesses or to file amicus curiae briefs.[128] The White House could call on Congress to pass robust privacy legislation, directing the FTC to enforce the FTC Act and protect privacy. The President should engage in the legislative arena,[129] enact executive policies to protect privacy,[130] and help mobilize interest groups.[131]

The government must have access to certain information, but rules governing access and practices should be public. Secret, unchallengeable demands threaten due process, prevent public debate, and invade our privacy. Secret policies and interpretations mean we cannot assess what political philosopher John Rawls called "justice as regularity"—"[t]he regular and impartial, and in this sense fair, administration of law."[132] If we do not know when, why, and how the government obtains and uses information, or is permitted to use information, how can we evaluate the justice of the government and its actions?

---

[127] *See, e.g.*, Garrett M. Graff, *Don't Know Their Yahoo from Their YouTube*, WASH. POST, Dec. 2, 2007, at B1 (quoting Senator John McCain's classification of "information technology" as a "less important issue[]"); Mike Masnick, *Supreme Court Justices Discuss Twitter*, TECHDIRT (May 25, 2010, 12:05 AM), http://www.techdirt.com/articles/20100521/1631459536 (revealing the lack of understanding Justices Scalia and Breyer have of Twitter); *Your Own Personal Internet*, WIRED (June 30, 2006, 12:47 AM), http://www.wired.com/threatlevel/2006/06/your_own_person/ (quoting U.S. Senator Ted Stevens referring to the internet as "a series of tubes").

[128] A novel solution is moving Camp David to Silicon Valley so the President and Senators can interact with technology and technologists. *See* Nigel Cameron, President, Ctr. for Policy on Emerging Techs., Jim Dempsey, Vice President for Pub. Policy, Ctr. for Democracy and Tech., Rebecca Lynn, Partner, Morgenthaler Ventures, Christine Peterson, President, Foresight Inst., David Tennenhouse, Partner, New Venture Partners, Conference Panel at the Tech Policy Summit and the Center for Policy on Emerging Technologies Breakfast, *Bridging the Continental Divide: From the Valley to D.C*, (Nov. 15, 2011), *available at* http://vimeo.com/32851257.

[129] The President could push for legislation to reverse or address court decisions that punt on important privacy questions. For example, in response to the Supreme Court's decision (not concerning privacy) in *Ledbetter v. Goodyear Tire & Rubber Co.*, 550 U.S. 618 (2007), President Barack Obama signed the Lilly Ledbetter Fair Pay Act of 2009, to restore the law to where it was before the Supreme Court's decision. Lilly Ledbetter Fair Pay Act of 2009, Pub. L. No. 111-2, § 2, 123 Stat. 5, 5.

[130] *See generally* Terry M. Moe & William G. Howell, *The Presidential Power of Unilateral Action*, 15 J.L. ECON. & ORG. 132, 132, 155 (1999).

[131] *See generally* Mark A. Peterson, *The Presidency and Organized Interests: White House Patterns of Interest Group Liaison*, 86 AM. POL. SCI. REV. 612, 615 (1992).

[132] RAWLS, *supra* note 34, at 207.

IV. CASE STUDY OF FTC ENFORCEMENT

Having reviewed where privacy has stalled legislatively and judicially, and having offered some potential solutions, I now turn to enforcement. In Part III, I focused on government abuses to privacy, and, in this Part, I deal with private abuses to privacy. In both arenas, abuses occur because of similar problems—poor laws, poor enforcement, and broken social expectations—that trigger all three aspects of my proposed privacy framework. In this case, Congress has charged the FTC and the Federal Communications Commission ("FCC") with regulating businesses and protecting consumers. Privacy laws, however, can be confusing and difficult to apply, especially to new technologies.[133] The agencies have tepidly retaliated against companies that have broken laws and violated our social expectations.[134] The lack of regulation sends mixed messages: if companies break the law and violate privacy, as the FTC claims and is evident, why are there no meaningful consequences, fines, or prosecutions? The FTC should exercise its litigation and compliance authorities, extract financial and business reparations from legal violators, and pursue criminal charges.

The Facebook[135] and Google[136] cases illustrate an FTC strategy also employed against MySpace,[137] Twitter,[138] and others. As matters stand, it is rational for prosecuted companies to settle and enter into a consent decree with the FTC,[139] thereby avoiding admittance of wrongdoing and fines.[140] In a consent decree, companies are required to develop privacy plans, submit to privacy reviews, seek their customers' permission before sharing their information, and pledge not to further misrepresent their

---

[133] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1048 (2010).

[134] *See, e.g.*, Comments from the Elec. Privacy Info. Ctr. to the Fed. Trade Comm'n 2 (Dec. 27, 2011), *available at* http://www.epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf ("[T]he proposed [settlement agreement with Facebook] is insufficient to address the concerns originally identified by EPIC and the consumer coalition, as well as those findings established by the [FTC].").

[135] Facebook, Inc., FTC No. 092 3184, at 1 (July 27, 2012) (providing a settlement agreement).

[136] Google, Inc., FTC No. 102 3136, at 1 (Oct. 13, 2011) (providing a settlement agreement).

[137] Myspace, LLC, FTC No. 102 3058, at 1 (Aug. 30, 2012) (providing a settlement agreement).

[138] Twitter, Inc., FTC No. 092 3093, at 1 (Mar. 2, 2011) (providing a settlement agreement).

[139] Malcolm B. Coate et al., *Fight, Fold or Settle?: Modelling the Reaction to FTC Merger Challenges*, 33 ECON. INQUIRY 537, 537, 550 (1995).

[140] *See, e.g.*, Facebook, Inc., 76 Fed. Reg. 75883, 75883 (Fed. Trade Comm'n Dec. 5, 2011) (analysis of proposed consent order) (settling "*alleged* violations of federal law" (emphasis added)).

privacy policies.[141] This requirement raises the unsettling question of whether the companies were previously permitted to misrepresent their policies.

Google and Facebook used and gathered information in a host of ways that violated their terms, privacy policies, and our broader social expectations. The absence of meaningful censure for these repeated offenses is a further violation of our social expectations. The Google Decree arose over the ways that Google Buzz shared information.[142] Then, Google Street View cars gathered e-mails, passwords, photos, chat messages, and sites visited from bystanders, even if users were not using a computer at the time.[143] Google blamed an engineer, but the practice was planned and known to supervisors.[144] Google later subverted Safari's "Do Not Track" features, despite user indications that they did not wish to be tracked.[145] Google claimed, "We didn't anticipate that this would happen."[146] Google altered its privacy policies in a widely criticized way that used users' information in a new fashion.[147] Google settled with the FCC for $25,000 after having "impeded" and "delayed" a federal inquiry;[148] this fine accounts for 0.000066% of their annual revenue of $37.9 billion.[149] Another $22.5 million settlement for subverting "do not track" features relative to the infraction and their revenue was a miniscule fine.[150] As it turns out, Google also kept the information they had gathered through Street View cars.[151]

---

[141] *See, e.g.*, Facebook, Inc., FTC No. 092 3184, at 3–6 (July 27, 2012); Google, Inc., FTC No. 102 3136, at 3–5.

[142] Complaint at 3–6, Google, Inc., FTC No. 102 3136.

[143] David Streitfeld & Kevin J. O'Brien, *Protecting Its Own Privacy: Inquiries on Street View Get Little Cooperation from Google*, N.Y. TIMES, May 23, 2012, at B1 (noting that Google Street View cars collected "e-mails, photographs, passwords, chat messages, postings on Web sites and social networks—all sorts of private Internet communications").

[144] David Streifeld, *Google Engineer Told Others of Data Collection, Full Version of F.C.C. Report Reveals*, N.Y. TIMES, Apr. 29, 2012, at A22.

[145] Statement of the Commission at 1, Google, Inc., FTC No. 102 3136.

[146] Heather Perlberg & Brian Womack, *Google Dodged iPhone Users' Privacy With DoubleClick, Stanford Study Finds*, BLOOMBERG (Feb. 17, 2012, 5:39 PM), http://www.bloomberg.com/news/2012-02-17/google-dodged-iphone-users-privacy-with-doubleclick-stanford-study-finds.html.

[147] Google began compiling tracked-user information across multiple sites including Gmail, YouTube, and its search engine; users were unable to opt out of the policy. Cecilia Kang, *Google to Track Users Across All Its Sites*, WASH. POST, Jan. 25, 2012, at A1.

[148] David Streitfeld, *Google Is Faulted for Impeding U.S. Inquiry on Data Collection*, N.Y. TIMES, Apr. 15, 2012, at A1.

[149] Brian Womack & Todd Shields, *Google Gets Maximum Fine After 'Impeding' Privacy Probe*, BLOOMBERG (Apr. 16, 2012, 2:32 PM), http://www.bloomberg.com/news/2012-04-15/fcc-seeks-25-000-fine-from-google-in-wireless-data-privacy-case.html.

[150] Claire Cain Miller, *Google, Accused of Skirting Privacy Provision, Is to Pay $22.5 Million to Settle Charges*, N.Y. TIMES, Aug. 10, 2012, at B2; *see also* Geoff Duncan, *Google's $22.5 Million FTC Penalty Is Not Enough: Here's Why*, DIGITAL TRENDS (July 10, 2012),

Facebook publicly displayed information users thought was private, allowed advertisers to gather users' personal information, and allowed access to users' information even if users deleted their profile.[152] The FTC called these practices "unfair and deceptive."[153] The FTC did not respond when Facebook tracked users who were logged out of their Facebook accounts[154] or when Facebook unveiled "Timeline," which shared information in new, intrusive ways.[155] Although these repeated privacy abuses may suggest otherwise, the FTC does have tools to respond to law-breakers, particularly once companies have entered consent agreements such as the ones Google and Facebook have with the FTC.

A. Solution: Enhanced Enforcement

The FTC has broad powers to investigate cases, bring complaints against companies, and punish lawbreakers.[156] The FTC Policy Statement on Deception says deception is a "representation, omission, or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[157] The FTC Act stipulates that "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[158] If a user is misled, the FTC can bring a civil action.[159] The FTC can assess penalties of $10,000 per violation of "unfair" and "deceptive" practices,[160] practices of the type Facebook and Google have employed. Although courts has prevented the government from imposing excessively large fines,[161] large fines may be exactly what

---

http://www.digitaltrends.com/mobile/googles-22-5-million-ftc-penalty-is-not-enough-heres-why/ ("[I]t's hard to believe any company trying to compete with Google or Facebook will consider dodgy privacy practices anything more than a minor cost of doing business.").

[151] Streitfeld, *supra* note 148.

[152] Somini Sengupta, *F.T.C. Settles Privacy Issue at Facebook*, N.Y. TIMES, Nov. 30, 2011, at B1.

[153] Complaint at 7, Facebook, Inc., FTC No. 092 3184 (July 27, 2012).

[154] Dina ElBoghdady & Hayley Tsukayama, *Facebook Tracking Probe Sought*, WASH. POST, Sept. 30, 2011, at A14.

[155] *Id.*

[156] *See, e.g.*, 15 U.S.C. §§ 45, 46(a), 49, 56, 57b-1 (2006).

[157] Cliffdale Associates, Inc., 103 F.T.C. 110, 176 (1984).

[158] § 45(a)(1); *see also* 12 C.F.R. § 227.1(b) (2012).

[159] § 45(m)(1)(A).

[160] *Id.* ("In such action, such person, partnership, or corporation shall be liable for a civil penalty of not more than $10,000 for each violation."); 16 C.F.R. § 1.98(d) (2012) (increasing the penalty under 15 U.S.C. § 45(m)(1)(A) (2006) from $10,000 to $16,000).

[161] *See, e.g.*, United States v. Bajakajian, 524 U.S. 321, 324 (1998) (holding that the imposed fine was unconstitutional under the Eighth Amendment).

is necessary to deter future misconduct.[162] The repeated occurrence of multiple privacy violations perpetrated on millions of Google and Facebook users could justify leveling substantial fines of the type that would attract companies' attention. One can imagine businesses reacting by accusing the FTC of unprecedented, anti-business practices, stifling creativity, or not understanding technology. However, breaking the law necessitates punishment.

In the past, the FTC has relied upon self-regulation—trying to provide consumers with access to information to protect their own privacy.[163] Critics of self-regulation tend to believe it does not work[164] or that it might work too well.[165] In a large group of companies, in which no individual contribution or lack thereof makes a notable difference, it is unlikely that a solution will emerge without coercion or exogenous factors.[166] As such, privacy self-regulation initiatives have often stalled or failed.[167]

---

[162] *See* BMW of N. Am., Inc. v. Gore, 517 U.S. 559, 568 (1996) ("Punitive damages may properly be imposed to further a State's legitimate interests in punishing unlawful conduct and deterring its repetition.").

[163] *See* Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 J.L. & POL'Y FOR INFO. SOC'Y 723, 729 (2007).

[164] *See generally id.* at 729–44.

[165] FTC Commissioner J. Thomas Rosch voiced this second concern, noting that although certain best practices are desirable, there is a danger in "large, well-entrenched firms engaging in 'self-regulation'" because it could lead to them "dictat[ing] what the privacy practices of their competitors should be." *Internet Privacy: The Views of the FTC, FCC, and NTIA: Testimony Before the Subcomm. on Commerce, Mfg. & Trade and Subcomm. on Commc'ns & Tech. of the H. Comm. on Energy & Commerce*, 112th Cong. 3 n.4 (2011) (statement of J. Thomas Rosch, Commissioner, FTC).

[166] MANCUR OLSON, JR., THE LOGIC OF COLLECTIVE ACTION 44 (1965).

[167] *See, e.g.*, PAM DIXON, WORLD PRIVACY FORUM, THE NETWORK ADVERTISING INITIATIVE: FAILING AT CONSUMER PROTECTION AND AT SELF-REGULATION 6–7 (2007). The Network Advertising Initiative ("NAI") is an FTC-supported example of "behavioral" advertising self-regulation. *Id.* at 2 ("[T]he agreement and the related self-regulatory body—called the Network Advertising Initiative or NAI—have failed to protect consumers and have failed to self-regulate the behavioral targeting industry."). In one study, however, only 11% of participants were able to determine the function of the NAI opt-out website. Aleecia M. McDonald & Lorrie Faith Cranor, *Americans' Attitudes About Internet Behavioral Advertising Practices*, WORKSHOP ON PRIVACY ELECTRONIC SOC'Y, Oct. 2010, at pt. 7 (pre-press version), *available at* http://www.aleecia.com/authors-drafts/wpes-behav-AV.pdf. The FTC found that, in the NAI, "[c]urrent membership constitutes over 90% of the network advertising industry in terms of revenue and ads served" and "only legislation can compel the remaining 10% of the industry to comply with fair information practice principles. Self-regulation cannot address recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program." FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS (PART 2): RECOMMENDATIONS 10 (2000). Another example is the Platform for Privacy Preferences ("P3P"), a self-regulatory mechanism for websites to communicate privacy policies to user agents. Thousands of websites use P3P compact policies to misrepresent their privacy practices. PEDRO GIOVANNI LEON ET AL.,

Perhaps the FTC fears that if it litigated a case and lost, its authority would erode. If so, the FTC should request that Congress pass legislation clarifying the extent to which online privacy violations are illegal and empowering the FTC to punish wrongdoers, and Congress should do so. Perhaps FTC commissioners are hindered by the lack of available technology.[168] Perhaps FTC commissioners, many of whom come from or go to the corporate world,[169] are concerned about future job prospects.[170] If that is the case, the Commission should consider appointing candidates less concerned about their post-Commission professional prospects.[171] Perhaps the FTC is under-staffed.[172] If so, it could request a larger staff. FTC Commissioners may genuinely believe in unbridled capitalism and worry that robust fines or regulations will

---

TOKEN ATTEMPT: THE MISREPRESENTATION OF WEBSITE PRIVACY POLICIES THROUGH THE MISUSE OF P3P COMPACT POLICY TOKENS 1 (2010).

[168] *See* Peter Maass, *How a Lone Grad Student Scooped the Government and What It Means for Your Online Privacy*, PROPUBLICA (June 28, 2012, 6:30 AM), http://www.propublica.org/article/how-a-grad-student-scooped-the-ftc-and-what-it-means-for-your-online-privac ("The desktop in their [FTC] office is digitally shackled by security filters that make it impossible to freely browse the Web. Crucial websites are off-limits, due to concerns of computer viruses infecting the FTC's network, and there are severe restrictions on software downloads. . . . Only one FTC official has an unfiltered desktop . . . ."). *But see* Kashmir Hill, *The FTC, 'Your Privacy Watchdog,' Does Have Some Teeth*, FORBES (Jun. 29, 2012, 4:21 PM), http://www.forbes.com/sites/kashmirhill/2012/06/29/your-privacy-watchdog-does-have-some-teeth (defending the FTC's capabilities in direct response to the ProPublica article).

[169] Former government employees frequently provide expert policy advice. *See* Kevin T. McGuire, *Lobbyists, Revolving Doors and the U.S. Supreme Court*, 16 J.L. & POL. 113, 120 (2000) ("[I]n the world of pressure politics, policy-makers reward those representatives who provide them with the types of reliable information that enable them to advance their respective goals."). I have examined this pattern as it relates to the Supreme Court. *See* Matthew L. Sundquist, *Learned in Litigation: Former Solicitors General in the Supreme Court Bar*, 5 CHARLESTON L. REV. 59, 60 (2010).

[170] For example, as of September 2012, Robert Pitofsky, former Chairman of the FTC, serves as Counsel at Arnold & Porter LLP; Timothy Muris, another former FTC Chairman, is Of Counsel to Kirkland & Ellis LLP; Pamela Jones Harbour, former FTC Commissioner, is a partner at Fulbright & Jaworski LLP; Deborah Platt Majoras, former FTC Chairman, is the CLO at Procter & Gamble; and Thomas Leary, former FTC Commissioner, is Of Counsel to Hogan Lovells.

[171] Officials elsewhere in the government have sought to reduce the revolving-door pattern by extending the no-lobbying period. *See* Close the Revolving Door Act of 2010, S. 3272, 111th Cong. § 5 (2010). The White House could look outside the corporate world for regulatory candidates and recruit policy experts, advocates, scholars and others less interested in a corporate job after their tenure. Congress could ban former regulators and staffers from lobbying, advocating, consulting, or representing companies governed by the agency they worked for, either indefinitely or for five to ten years.

[172] *See* Maass, *supra* note 168 ("The mismatch between FTC aspirations and abilities is exemplified by its Mobile Technology Unit, created earlier this year to oversee the exploding mobile phone sector. The six-person unit consists of a paralegal, a program specialist, two attorneys, a technologist and its director . . . .").

discourage innovation or competition.[173] Regardless, as the World Privacy Forum points out, the unfortunate reality is that "companies that are the target of Commission actions know that the penalties are often weak in comparison to the profits, and that it is more cost-effective to exploit consumers today and say that they are sorry tomorrow if they are caught."[174]

B. Coalition Solutions

Given that legislation and self-regulation are unlikely to be sufficiently successful tactics for privacy protection, and given that the FTC can serve as a successful but necessarily limited agent for privacy enforcement, this Section considers another strategic approach. Stakeholders in business, technology, government, and consumer protection have advocated better privacy or created privacy frameworks that can be realized through standardized agreements. None are perfect, but they are a good start. In essence, there are two distinct problems to address. First, how should we lobby Congress, corporations, and other politicians to implement and enforce meaningful privacy policies? Second, in the absence of effective lobbying, or perhaps as a supplement, how can we promote effective behavior among users and businesses? Education is a crucial factor, and advocacy must come from all stakeholders.

A handful of allied government, industry, and advocacy groups have defined "best practices," supported responsible data usage, and advocated privacy in the cloud, many of them calling for ECPA reforms.[175] Government-led coalitions have already begun to leverage their organizational capacity.[176] Cisco, SAP, EMC, and others have

---

[173] *See* FED. TRADE COMM'N, TO PROMOTE INNOVATION: THE PROPER BALANCE OF COMPETITION AND PATENT LAW AND POLICY 1 (2003) ("Competition through free enterprise and open markets is the organizing principle for most of the U.S. economy. Competition among firms generally works best to achieve optimum prices, quantity, and quality of goods and services for consumers.").

[174] Dixon, *supra* note 12, at 2.

[175] *See generally* COMPUTER & COMMC'NS INDUS. ASS'N, PUBLIC POLICY FOR THE CLOUD: HOW POLICYMAKERS CAN ENABLE CLOUD COMPUTING 22–35 (2011); CONSUMER FED'N OF AM., CONSUMER PROTECTION IN CLOUD COMPUTER SERVICES: RECOMMENDATIONS FOR BEST PRACTICES 5–6 (2010); INDUSTRY RECOMMENDATIONS ON THE ORIENTATION OF A EUROPEAN CLOUD COMPUTING STRATEGY (2011); OPEN IDENTITY EXCH., AN OPEN MARKET SOLUTION FOR ONLINE IDENTITY ASSURANCE 9 (2010); TECHAMERICA FOUND., SUMMARY REPORT OF THE COMMISSION ON THE LEADERSHIP OPPORTUNITY IN U.S. DEPLOYMENT OF THE CLOUD (CLOUD²) 2–3, 6 (2011).

[176] The White House has advocated for a Consumer Privacy Bill of Rights, identifying a "need for transparency to individuals about how data about them is collected, used, and disseminated and the opportunity for individuals to access and correct data that has been collected about them." THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING

embraced an Open Cloud Manifesto supporting standardization based on customer requirements.[177] The cloud-computing industry has created semi-standardized privacy policies and practices in the form of End User License Agreements ("EULA"),[178] Terms of Services, and Service Level Agreements. These may be informative,[179] but they are infrequently read and difficult to understand.[180] Best practices for information security management have also been defined by the international information security standard known as ISO/IEC 27001 and 27002,[181] though they remain imperfect.[182] For these groups to be successful, they will need to find broad areas of agreement where they can pursue specific, tangible goals as the coalition opposing the Stop Online Piracy Act did.

INNOVATION IN THE GLOBAL DIGITAL ECONOMY 13 (2012). The National Strategy for Trusted Identities in Cyberspace ("NSTIC") is another White House initiative to work with companies, advocacy groups, and agencies to improve online privacy. The Strategy calls for inter-operable technology where people, companies, and technology can be authenticated. The idea is to create a system wherein individuals could choose to securely validate their identities when necessary. *See About NSTIC*, NAT'L STRATEGY TRUSTED IDENTITIES CYBERSPACE, http://www.nist.gov/nstic/about-nstic.html (last visited Oct. 17, 2012); *see also* THE WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE 2 (2011).

[177] *Clash of the Clouds*, ECONOMIST, Apr. 4, 2009, at 66, 66. Amazon, Google, Microsoft, and Salesforce.com did not join, demonstrating how far away industry agreement may be. *Id.* at 67; s*ee also* OPEN CLOUD MANIFESTO (2009), *available at* http://www.opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf.

[178] *See* Jens Grossklags & Nathan Good, *Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 341 (Sven Dietrich & Rachna Dhamija eds., 2007).

[179] *See* Robert W. Gomulkiewicz & Mary L. Williamson, *A Brief Defense of Mass Market Software License Agreements*, 22 RUTGERS COMPUTER & TECH. L.J. 335, 346–52 (1996).

[180] Balachandra Reddy Kandukuri et al., *Cloud Security Issues*, *in* 2009 IEEE INT'L CONF. ON SERVICES COMPUTING 517, 519 (2009); *see also* Grossklags & Good, *supra* note 178 (noting the length of software program EULAs averaged at eleven double-spaced pages); Turow, *supra* note 163.

[181] *See Security Zone: Promoting Accountability Through ISO/IEC 27001 & 27002 (Formerly ISO/IEC 17799)*, COMPUTER WKLY. (Dec. 2008), http://www.computerweekly.com/feature/Security-Zone-Promoting-accountability-through-ISO-IEC-27001-27002-formerly-ISO-IEC-17799; *see also* Thomas J. Smedinghoff, *It's All About Trust: The Expanding Scope of Security Obligations in Global Privacy and E-Transactions Law*, 16 MICH. ST. J. INT'L L. 1, 41–42 (2007) ("This [ISO/IEC 27001] standard . . . defines the requirements for an Information Security Management System (ISMS) and provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS.").

[182] *See* Smedinghoff, *supra* note 181, at 42 (noting that ISO/IEC 27001 is a good starting point for security but "does not guarantee legal compliance"); *ISO/IEC 27002*, ISO 27001 SECURITY, http://www.iso27001security.com/html/27002.html (last visited Sept. 2, 2012) (acknowledging the difficulties in assessing whether an organization has complied with ISO/IEC 27002 standards).

C. Lessons from the Collaboration Against SOPA

The multi-stakeholder process to prevent the Stop Online Piracy Act ("SOPA")[183] is a useful template for a privacy coalition. SOPA would make internet service providers responsible for filtering copyright infringement material, targeting those who enable or facilitate copyright infringement.[184] Commentators argued that Google, YouTube, and other sites could be blocked, while some claimed it would lead to an internet "blacklist"[185] or a "great firewall of America."[186] Nonetheless, the deck was stacked in favor of SOPA. Well-established players in the industry enjoy better financing, established organization, and superior institutional knowledge and relationships.[187] As the president of the Computer and Communications Industry Association pointed out, "If you are a member of the Judiciary Committee, year after year after year, the content industry has been at your fundraisers over and over."[188] Organizations supporting SOPA had given nine times as much money to members of Congress as organizations in opposition.[189] Indeed, Representative Lamar Smith, the sponsor, called just one opposition witness at the House Judiciary Committee; he called five supportive witnesses.[190] The Center for Democracy and Technology and the Electronic Frontier Foundation were initial opponents of SOPA, but soon more stakeholders joined a coalition organizing "American Censorship Day," supported by Mozilla, Wikimedia, and others.[191] Google, AOL, and

---

[183] Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011).

[184] *Id.* § 103.

[185] David Carr, *The Danger of an Attack on Piracy Online*, N.Y. TIMES, Jan. 2, 2012, at B1.

[186] Rebecca MacKinnon, Op-Ed., *Stop the Great Firewall of America*, N.Y. TIMES, Nov. 15, 2011, http://www.nytimes.com/2011/11/16/opinion/firewall-law-could-infringe-on-free-speech.html?_r=0.

[187] Jennifer Martinez, *Shootout at the Digital Corral*, POLITICO (Nov. 16, 2011, 4:31 AM), http://www.politico.com/news/stories/1111/68448.html.

[188] *Id.*

[189] *H.R. 3261 - Stop Online Piracy Act (SOPA)*, MAPLIGHT, http://www.maplight.org/us-congress/bill/112-hr-3261/1019110/total-contributions.table (last visited Aug. 27, 2012).

[190] Will Oremus, *The Rise of the Geek Lobby*, SLATE (Nov. 30, 2011, 8:02 PM), http://www.slate.com/articles/technology/technocracy/2011/11/stop_online_piracy_act_can_the_geek_lobby_stop_hollywood_from_wrecking_the_internet_.html; *see also Online Piracy: Stopping SOPA*, ECONOMIST, Jan. 21, 2012, at 33, 33.

[191] Kristen Salyer, *'American Censorship Day' Makes an Online Statement: The Ticker*, BLOOMBERG (Nov. 16, 2011, 5:02 PM), http://www.bloomberg.com/news/2011-11-16/-american-censorship-day-makes-an-online-statement-the-ticker.html; *see also American Censorship Day: Nov. 16, 2011*, AM. CENSORSHIP DAY, http://americancensorship.org (last visited Oct. 17, 2012); FIGHT FOR THE FUTURE, http://fightforthefuture.org (last visited Oct. 17, 2012).

Facebook criticized SOPA in a full-page *New York Times* ad.[192] The Twitter hashtag "DontBreakTheInternet" trended upwards, and 87,000 people called Congress to voice their opposition in one day.[193] President Obama then publicly opposed SOPA.[194] Continued work on the bill was indefinitely delayed.[195]

SOPA showed a moment of unity, but in privacy, everyone has varied interests. Consumers have different views of privacy than do businesses and governments. Opposing legislation is quite different from formulating ideas and advocating policy positions or legislation. However, as the anti-SOPA group and groups like the Future of Privacy Forum and Digital Due Process Coalition demonstrate,[196] there are areas where stakeholders can work together. Social media is empowering in this regard, as is calling Congress, signing petitions,[197] and, on an individual level, filing complaints with the FTC,[198] FCC,[199] and your attorney general or governor.[200] I file as often as I find privacy infringements or misleading terms or policies, and I encourage others to do likewise.

---

[192] *We Stand Together to Protect Innovation*, N.Y. TIMES, Nov. 16, 2011, at A11 ("[T]he bills as drafted would expose law-abiding U.S. Internet and technology companies to new and uncertain liabilities, private rights of action, and technology mandates that would require monitoring of websites. We are concerned that these measures pose a serious risk to our industry's continued track record of innovation and job creation, as well as to our nation's cybersecurity.").

[193] Oremus, *supra* note 190.

[194] Edward Wyatt, *White House Takes Issue with 2 Antipiracy Bills*, N.Y. TIMES, Jan. 15, 2012, at A22.

[195] Jonathan Weisman, *Antipiracy Bills Delayed After an Online Firestorm*, N.Y. TIMES, Jan. 21, 2012, at B6.

[196] The Future of Privacy Forum is a D.C.-based think tank that brings together privacy advocates from academia, technology, business, and consumer protection. *Our Mission*, FUTURE OF PRIVACY F., http://www.futureofprivacy.org/about/our-mission/ (last visited Oct. 17, 2012). The Digital Due Process Coalition is a group of business and advocacy groups that advocate amending the ECPA. *See About the Issue*, DIGITAL DUE PROCESS COALITION, http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Oct. 17, 2012).

[197] Issue-specific petitions have been compiled in this vein. *See, e.g.*, NOT WITHOUT A WARRANT, https://notwithoutawarrant.com (last visited Oct. 17, 2012) (advocating amending the ECPA).

[198] *See Before You Submit a Complaint,* FED. TRADE COMMISSION, https://www.ftccomplaintassistant.gov (last updated Aug. 1, 2012, 9:30 AM).

[199] *See File Complaint*, FED. COMM. COMMISSION, http://www.fcc.gov/complaints (last visited Oct. 17, 2012).

[200] *See, e.g.*, *Consumer Alerts, Information & Complaints*, CAL. DEP'T JUST., http://oag.ca.gov/consumers/general (last visited Oct. 17, 2012).

CONCLUSION

In the short term, education is needed to inform users of privacy practices and allow them to determine if their expectations are realistic, in tune with the law, and enforced. Advocacy groups have written helpful educational materials.[201] The FTC has shown exceptional energy in educating consumers, leading industry discussions, and advocating that companies promote privacy.[202] Once society understands and is eager to fix these problems, we can set off fire-alarms, putting our representatives on notice that we value the social contract and that privacy is a highly valued good.

Kinakuta, a fictional island in the science fiction novel *Cryptonomicon*, is used to traffic data outside legal regulations.[203] A large corporation with the will-power and financing could theoretically create a floating data center, beyond government reach or user

---

[201] *See, e.g.*, *Fact Sheet 18: Online Privacy: Using the Internet Safely*, PRIVACY RTS. CLEARINGHOUSE (last updated Aug. 2012), https://www.privacyrights.org/fs/fs18-cyb.htm; *Getting Started: Web Site Privacy Policies*, CENTER FOR DEMOCRACY & TECH., https://www.cdt.org/privacy/guide/start/privpolicy.php (last visited Oct. 17, 2012). "Disconnect" is a browser extension that prevents major third parties and search engines from tracking users' online activity. DISCONNECT, http://disconnect.me/db/ (last visited Oct. 17, 2012). An iPhone tracker visualizes what information can be gleaned from the files on your phone. IPHONE TRACKER, http://petewarden.github.com/iPhoneTracker/ (last visited Oct. 17, 2012). "Take This Lollipop" is a short video that, using Facebook Connect, depicts a crazed man stalking you in Facebook, revealing the extent of your personal information available online. *JARRETTHOLT2*, *Take This Lollipop*, YOUTUBE (Nov. 3, 2011), http://www.youtube.com/watch?v=1pA_UatfFW0. In general, Facebook applications can access an incredible amount of information. *See Permissions Reference*, FACEBOOK, http://developers.facebook.com/docs/authentication/permissions/ (last visited Aug. 22, 2012). Pleaserobme.com combines information from Foursquare and Twitter to identify when people have willingly provided their location information. Dan Fletcher, *Please Rob Me: The Risks of Online Oversharing*, TIME BUS., Feb. 18, 2010, http://www.time.com/time/business/article/0,8599,1964873,00.html. Ghostery blocks cookies and displays which cookies have tracked you. GHOSTERY, http://www.ghostery.com (last visited Oct. 17, 2012). Similar programs have minimal effectiveness. Jonathan Mayer, *Tracking the Trackers: Self-Help Tools*, CENTER FOR INTERNET & SOC'Y (Sept. 13, 2011, 4:35 AM), http://cyberlaw.stanford.edu/node/6730 ("Most desktop browsers currently do not support effective self-help tools."). The Electronic Frontier Foundation has a project to demonstrate to users all the information computers transmit to websites. *See* PANOPTICLICK, https://panopticlick.eff.org/ (last visited Oct. 17, 2012).

[202] *See, e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 14 (2012).

[203] *See generally* NEAL STEPHENSON, CRYPTONOMICON (1999). In a real-world comparison, an abandoned WWII Fortress island off the coast of England, "Sealand," nearly became a data center targeting customers looking for complete freedom from government. *See* James Grimmelmann, *Sealand, HavenCo, and the Rule of Law*, 2012 U. ILL. L. REV. 405, 406–07 (2012).

protection.[204] Given the legal gray area surrounding founding countries[205] and data storage in space,[206] it is not inconceivable to imagine a corporation or group of individuals creating a real-world Kinakuta where information that threatens or violates our privacy could be gathered, processed, and exploited. Corporations, however, need not resort to the safety of clandestine islands: privacy violations happen on our own shores, but quietly, secretly, and beyond the scope of challenge or knowledge. And they occur brazenly, in the open, when laws are sufficiently vague or poorly enforced so that companies and the government need not establish a physical haven. Their havens are ignorance, obfuscation, secrecy, complacency, and confusion.

---

[204] *See* Paul T. Jaeger et al., *Where is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing*, FIRST MONDAY (May 4, 2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2456/2171.

[205] *See* Doug Bandow, *Getting Around Big Government: The Seastead Revolution Begins to Take Shape*, FORBES (July 20, 2012, 9:45 AM), http://www.forbes.com/sites/dougbandow/2012/07/30/getting-around-big-government-the-seastead-revolution-begins-to-take-shape (discussing the vision to create a floating city beyond any country's jurisdiction). *See generally* JEROME FITZGERALD, SEA-STEADING: A LIFE OF HOPE AND FREEDOM ON THE LAST VIABLE FRONTIER (2006).

[206] *See* Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 610 U.N.T.S. 206. *See generally* MYRES S. MCDOUGAL ET AL., LAW AND PUBLIC ORDER IN SPACE (1963); GEORGE S. ROBINSON & HAROLD M. WHITE, JR., ENVOYS OF MANKIND: A DECLARATION OF FIRST PRINCIPLES FOR THE GOVERNANCE OF SPACE SOCIETIES (1986); Barton Beebe, Note, *Law's Empire and the Final Frontier: Legalizing the Future in the Early* Corpus Juris Spatialis, 108 YALE L.J. 1737 (1999).