INTRODUCTION

A host of laws and regulations engage with the legal, technological, and social meanings of privacy. In a country of more
than 300 million people⁴ 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,


³ Scholars have often advocated balanced frameworks for interpreting and protecting privacy. See JUDITH WAGNER DÉCÉW, IN PURSUIT OF PRIVACY: LAW, ÉTHICS, AND THE RISE OF TECHNOLOGY 75–78 (1997) (arguing that privacy entails informational privacy, accessibility privacy, and expressive privacy); JOHN PALFREY & ÚRS 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 perceptions 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, DÉDALUS, 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).

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.”).


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, while in the process contributing to the growth of a massive online-tracking industry. 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. 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 and has failed to examine whether texting on two-way pagers is private. Additionally, Congress has not updated key privacy legislation 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.


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).


17 See discussion infra Part III.B.
“secret interpretations” of the Patriot Act. Regulatory agencies have accepted trivial concessions and non-financial settlements from companies charged with breaking the law. Meanwhile, leaders struggle to grasp technology, and election-focused politicians prefer solving problems to preventing them as this yields greater credit from constituents.

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. 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.” But why is privacy so valuable and important? 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. It is, however,

---

19 See discussion infra Part IV.
20 See discussion infra Part III.C.
21 See discussion infra Part IV.
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, let alone to quantify its risks or benefits. 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. 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.”

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. 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.

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

---


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, we trade the state of nature—the world without government—to form a society and enjoy protection, security, and property. 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.” The law should serve the common interest and secure values that will be broadly useful to society. Once established, the law (and associated rules) must be enforced 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.”).


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. 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.

The third prong of my privacy framework values social expectations. Norms and expectations allow people to feel secure and ensure that society functions well. 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.” Problematically, technological limitations change and disappear quickly, allowing information to flow without the guidance of current expectations or social, ethical, legal, and political norms. 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.”).
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.\textsuperscript{41} Today, nearly half of American adults use smartphones.\textsuperscript{42} In 2014, mobile data usage is projected to be at 3,506% of what it was in 2009.\textsuperscript{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.”\textsuperscript{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,\textsuperscript{45} while Apple,\textsuperscript{46} Verizon,\textsuperscript{47} Target,\textsuperscript{48} and others\textsuperscript{49} compile

\textsuperscript{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/estats2010/2010reportfinal.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).


\textsuperscript{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 . . . ”).

\textsuperscript{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.”).

\textsuperscript{48} Charles Duhigg, Post, 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.”

It is estimated that 854,000 people hold top-secret security clearances. Using a GPS device, police can do what would have formerly required “a large team of agents, multiple vehicles, and perhaps aerial assistance.” As a result, technology untested by law has flourished—examples include respawning cookies, beacons and flash cookies, and browser-history sniffing. Governments and businesses build around new, unregulated technology and practices and then claim that changes would endanger their business or national security.

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. 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.


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. Privacy decision-
making and privacy features are also incredibly complex. Users cannot
research these settings under reasonable circumstances, much less
choose between them. In a recent study of forty-five experienced web-
users, participants were instructed to activate browsers and tools to
block cookies. Users blocked much less than they thought they did,
often blocking nothing. Users were unable to apply tools designed for
privacy, while companies and governments creating technological, legal,
and societal defaults aim to gather information. Behavioral economics
offers insight into these problems. 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.” 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,” 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
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
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
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).
guaranties. 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. 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.’”

We do expect that certain technology will not be used to exploit, expose, or abuse our privacy. Federal courts have occasionally protected these expectations as they relate to government activity, 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 Knots*? 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.”).


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.
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).
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-2003-05.pdf.
85 United States v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983).
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. 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 . . .” 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. 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. The Privacy Act has about a


89 Julia Angwin, Watchdog Planned for Online Privacy, WALL ST. J. (Nov. 11, 2010, 8:03 PM), http://online.wsj.com/article/SB100014240527487038482045756089701711176014.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).


91 Id. § 552a(b).


dozen exceptions,\textsuperscript{94} including a widely-criticized,\textsuperscript{95} broad exemption for “routine use.”\textsuperscript{96} There is little wonder it has been called “toothless.”\textsuperscript{97}

The Electronic Communications Privacy Act of 1986\textsuperscript{98} (“ECPA”) was drafted to protect the communication privacy of American citizens.\textsuperscript{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.\textsuperscript{100} Unnecessarily complex and overly technical distinctions—for instance, between opened and unopened email and email in transit and in storage—have emerged.\textsuperscript{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.\textsuperscript{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

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


\textsuperscript{96} § 552a(b)(3).


\textsuperscript{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.”).

\textsuperscript{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.”).

\textsuperscript{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.”).

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 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).
105 § 2709(b)(1).
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.”).
follow is the “police-patrol” model, which is “centralized, active, and direct.” Congress would pro-actively search for and remedy violations of its legislative goals. Congress, however, seems to prefer a “fire-alarm” model that forces citizens and advocacy groups to bear the costs of detection. 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. Legislators can then solve the problems, taking credit from those who sounded the alarm. 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, and congressional members’ interests in re-election can discourage active involvement in improving privacy policy. 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. 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


112 McCubbins & Schwartz, supra note 111, at 166.
113 Id.
114 Id. at 168.
115 Id. at 166.
116 Id. at 168.
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\textsuperscript{120} will likewise fail to protect privacy.\textsuperscript{121}

D. Looking Ahead

Senators, scholars, and advocates have asserted that agencies are infringing on our privacy.\textsuperscript{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.\textsuperscript{123} Congress must handle this type of large-scale public problem legislatively.\textsuperscript{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.\textsuperscript{125} It should empower courts and administrative agencies to revisit these issues. As necessary, it should redefine and amend legislative goals,\textsuperscript{126} particularly in areas of abused or subverted legislation. Where the Department of

\textsuperscript{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.”).


\textsuperscript{122} See, e.g., Privacy Online, supra note 3, at 33, 41; Wyden & Udall, supra note 18.

\textsuperscript{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.”).


\textsuperscript{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, Congress could rely on technologists when creating legislation, and courts could call on experts as witnesses or to file amicus curiae briefs. 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, enact executive policies to protect privacy, and help mobilize interest groups.

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.” 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/20100525/1631459536 (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 Tennenhause, 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.


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 Facebook135 and Google136 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

---

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].”).
137 Myspace, LLC, FTC No. 102 3058, at 1 (Aug. 30, 2012) (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, 550 (1995).
privacy policies. 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. Then, Google Street View cars gathered e-mails, passwords, photos, chat messages, and sites visited by bystanders, even if users were not using a computer at the time. Google blamed an engineer, but the practice was planned and known to supervisors. Google later subverted Safari’s “Do Not Track” features, despite user indications that they did not wish to be tracked. Google claimed, “We didn’t anticipate that this would happen.” Google altered its privacy policies in a widely criticized way that used users’ information in a new fashion. Google settled with the FCC for $25,000 after having “impeded” and “delayed” a federal inquiry; this fine accounts for 0.000066% of their annual revenue of $37.9 billion. Another $22.5 million settlement for subverting “do not track” features relative to the infraction and their revenue was a miniscule fine. As it turns out, Google also kept the information they had gathered through Street View cars.

---

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”).
145 Statement of the Commission at 1, Google, Inc., FTC No. 102 3136.
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.
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. The FTC called these practices "unfair and deceptive." The FTC did not respond when Facebook tracked users who were logged out of their Facebook accounts or when Facebook unveiled "Timeline," which shared information in new, intrusive ways. 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. 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." The FTC Act stipulates that “unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.” If a user is misled, the FTC can bring a civil action. The FTC can assess penalties of $10,000 per violation of “unfair” and “deceptive” practices, practices of the type Facebook and Google have employed. Although courts have prevented the government from imposing excessively large fines, 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.
155 Id.
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. 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. Critics of self-regulation tend to believe it does not work or that it might work too well. 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. As such, privacy self-regulation initiatives have often stalled or failed.

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.”).


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 Comm'n's & Tech. of the H. Comm. on Energy & Commerce, 112th Cong. 3 n.4 (2011) (statement of J. Thomas Rosch, Commissioner, FTC).


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.\textsuperscript{168} Perhaps FTC commissioners, many of whom come from or go to the corporate world,\textsuperscript{169} are concerned about future job prospects.\textsuperscript{170} If that is the case, the Commission should consider appointing candidates less concerned about their post-Commission professional prospects.\textsuperscript{171} Perhaps the FTC is under-staffed.\textsuperscript{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

\begin{flushright}
\textit{Token Attempt: The Misrepresentation of Website Privacy Policies Through the Misuse of P3P Compact Policy Tokens 1 (2010).}
\end{flushright}


\textsuperscript{169} Former government employees frequently provide expert policy advice. See Kevin T. McGuire, \textit{Lobbyists, Revolving Doors and the U.S. Supreme Court}, 16 J.L. & Pol. 113, 120 (2000) (“In 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, \textit{Learned in Litigation: Former Solicitors General in the Supreme Court Bar}, 5 Charleston L. Rev. 59, 60 (2010).

\textsuperscript{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.

\textsuperscript{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.

\textsuperscript{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.\textsuperscript{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.”\textsuperscript{174}

\textbf{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.\textsuperscript{175} Government-led coalitions have already begun to leverage their organizational capacity.\textsuperscript{176} Cisco, SAP, EMC, and others have

\begin{footnotesize}

\textsuperscript{174} Dixon, \textit{supra} note 12, at 2.


\textsuperscript{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.” \textit{The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting}
\end{footnotesize}
embraced an Open Cloud Manifesto supporting standardization based on customer requirements.\textsuperscript{177} The cloud-computing industry has created semi-standardized privacy policies and practices in the form of End User License Agreements ("EULA").\textsuperscript{178} Terms of Services, and Service Level Agreements. These may be informative,\textsuperscript{179} but they are infrequently read and difficult to understand.\textsuperscript{180} Best practices for information security management have also been defined by the international information security standard known as ISO/IEC 27001 and 27002,\textsuperscript{181} though they remain imperfect.\textsuperscript{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.


\textsuperscript{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).


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


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


\(^{184}\) Id. § 103.


\(^{188}\) Id.


Facebook criticized SOPA in a full-page New York Times ad.\textsuperscript{192} The Twitter hashtag “DontBreakTheInternet” trended upwards, and 87,000 people called Congress to voice their opposition in one day.\textsuperscript{193} President Obama then publicly opposed SOPA.\textsuperscript{194} Continued work on the bill was indefinitely delayed.\textsuperscript{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,\textsuperscript{196} there are areas where stakeholders can work together. Social media is empowering in this regard, as is calling Congress, signing petitions,\textsuperscript{197} and, on an individual level, filing complaints with the FTC,\textsuperscript{198} FCC,\textsuperscript{199} and your attorney general or governor.\textsuperscript{200} I file as often as I find privacy infringements or misleading terms or policies, and I encourage others to do likewise.

\textsuperscript{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.”).

\textsuperscript{193} Oremus, supra note 190.


\textsuperscript{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).


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. The FTC has shown exceptional energy in educating consumers, leading industry discussions, and advocating that companies promote privacy. 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. A large corporation with the will-power and financing could theoretically create a floating data center, beyond government reach or user

---


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

protection. Given the legal gray area surrounding founding countries and data storage in space, 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.

---

