Draft of 4/2/10

To be published in the *Stanford Law Review* (Fall 2010) as

"Privacy on the Books and on the Ground"

REGULATING FOR PRIVACY

Kenneth A. Bamberger & Deirdre K. Mulligan

Abstract

The sufficiency of U.S. information privacy laws—the regulations that govern companies' treatment of personally-identifiable data and information is the subject of heated debate. In in the view of a majority of privacy scholars and advocates, it fares poorly in contrast to the European regulatory framework.

Specifically, this group criticizes the existing patchwork of sectoral-based U.S. laws for failing to ensure across-the-board conformity with the standard measure of privacy protection: compliance with Fair Information Practice Principles (FIPPS) first articulated in the early 1970s. Such principles emphasize the provision of largely-procedural mechanisms, like notice and consent, intended to ensure individual "self-determination" over ones information. By contrast, EU member-state regimes are more often characterized by "omnibus" privacy laws: comprehensive codes governing all market actors uniformly, enforced by dedicated privacy agencies, and embodying full robust FIPPS procedural protections.

The positive critique of U.S. law may be correct—U.S. law is fragmented, incomplete, and often provides only limited procedures for controlling the use of ones information. Yet, we argue, the debate generates more heat than light as to the protection of substantive privacy goals, because it largely avoids sustained inquiry into the ways that U.S. law actually works, and how it combines with other forces to shape corporate privacy practices.

Our project seeks to fill that gap. We begin by exploring the findings and conclusions derived from the initial phase of an empirical study of privacy practices in U.S. corporations: semi-structured qualitative interviews with the 9 Chief Privacy Officers identified as leaders by their peers in the informational privacy community.

Spurred by these findings, we present a descriptive account of U.S. privacy regulation that upends the terms of the prevailing policy debate. Our alternative account identifies elements neglected by the traditional story—the emergence of the Federal Trade Commission as a privacy regulator, the increasing influence of privacy advocates, market and media pressures for privacy-protection, and the rise of privacy professionals—and traces the ways in which these players supplemented a privacy debate largely focused on processes (such as notice and consent mechanisms) with a growing corporate emphasis on substance: preventing violations of consumers' expectations of privacy.

This account has profound implications for debates about both privacy law's substance, and its form. As to the first: While bolstered procedural mechanisms for enhancing individual choices might be needed, pursuing that goal in a way that eclipses robust substantive protections, or constrains the regulatory flexibility that permits their evolution, will destroy important tools for overcoming corporate over-reaching, consumer manipulation, and the collective action problems raised by ceding privacy protection to individual choice alone.

As to the second: While the dominant account argues for greater uniformity and specificity in privacy law, the account on the ground suggests the value of governing privacy through flexible principles. Where Smith saw legal ambiguity as a "bug," we see it as a "feature." Our account describes how a regulator's entrepreneurial deployment of a broad and imprecise legal mandate centered a robust multi-player discourse about privacy that has focused market pressure and executive resources. The increase in corporate time and attention accorded to privacy, in turn, arose because, rather than in spite, of regulatory ambiguity.

REGULATING FOR PRIVACY

Kenneth A. Bamberger* & Deirdre K. Mulligan**

TABLE OF CONTENTS

* Assistant Professor of Law, University of California, Berkeley, School of Law (Boalt Hall).

** Assistant Professor, University of California, Berkeley, School of Information.

This project has been funded by the Rose Foundation for Communities and the Environment Consumer Privacy Rights Fund, and by TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422). We are extremely appreciative for critical assistance from Jen King and David Thaw; for important feedback from Catherine Albiston, Anita Allen, Colin Bennett, Beckwith Burr, Mary Culnan, Lauren Edelman, Chris Hoofnagle, Bob Kagan, Colin Koopman, David Medine, Maryanne McCormick, Helen Nissenbaum, Richard Purcell, Ira Rubinstein, Pamela Samuelson, Jason Schultz, Ari Schwartz, Paul Schwartz, Jeff Sovern, Peter Swire, Eric Talley, and other participants in workshops at the 2009 Privacy Law Scholars Conference, the UC Berkeley Center for the Study of Law and Society, the University of San Diego Law School, and the NYU School of Law Information Law Institute; and for excellent research assistance by April Elliot and Andy Weiner.

REGULATING FOR PRIVACY

INTRODUCTION

Fifteen years ago, management scholar H. Jeff Smith released a landmark study of corporate privacy practices,[1] and his conclusions were grim. In the seven corporations studied, the privacy arena was marked by systemic inattention, and lack of resources. "[P]olicies in important areas" were "non-existent," and those that existed were not followed in practice.[2] Executive neglect signaled to employees that privacy was not a strategic corporate issue. Privacy decisions were left to mid-level managers who lacked substantive expertise, played "particularly subservient roles in most privacy discussions"[3] and responded, piecemeal, to issues as they arose. Privacy considerations were particularly absent in decisions about technological or business developments; in the words of one mid-level manager, "[t]he top executives rarely ask for [privacy] policy implications of . . . new uses of information. If anybody worries about that, it's my [mid-level] colleagues and myself. And we don't usually know the right answer, we just try something."[4]

Smith attributed these failures to "ambiguity" regarding the legal meaning of privacy and the requirements governing its protection in the context of corporate data management.[5] In the face of this ambiguity corporate executives avoided action unless external parties demanded specific new policies and practices, a tendency exacerbated because privacy was viewed as a goal in tension with core operational aims—an organizational phenomena exacerbated by the inherent secrecy around corporate data management.

These findings led Smith to conclude that remedying the problem of corporate inattention to privacy concerns required a "systemic fix,"[6] reflecting an ongoing credible threat of either consumer backlash or government scrutiny. More concretely, he argued, the primary objective of regulatory intervention must be "the reduction of ambiguity in the U.S. privacy domain."[7] In light of these objectives—comprehensive, credible and unambiguous external mandates—Smith advocated a suite of reforms reflecting elements of the European approach to privacy protection.[8] He called for the adoption of a uniform

---

[1] H. JEFF SMITH, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA (1994).

[2] *Id.* at 4 (documenting "a persistent policy/practice gap").

[3] *Id.*

[4] *Id.* at 82.

[5] *See id.* at 139; ch. 5.

[6] *Id.* at 207.

[7] Id. at 213; *see id.* at ch. 6 (describing "Ambiguity All Around").

[8] Specifically Smith recommended a Data Protection Board with advisory powers to assist corporations in developing codes of acceptable practice, pursuant to a codified set of principles developed through consultation with industry, and field complaints. *See id.* at 207-224.

set of principles and a framework of more individualized industry codes, based on "Fair Information Privacy" principles (FIPPS)—an approach that emphasizes vindication of individual rights through mechanisms like notice and consent in decisions about the use of personal information—and he advocated the creation of a dedicated government board to assist in their implementation.[9] These steps, he concluded, would be necessary to force corporations to devote effective attention to privacy, as had happened with environmental protection.[10]

Smith's concerns have been echoed loudly for fifteen years. The dominant critique by privacy scholars and advocates charges that the U.S. system fails to provide adequate privacy protection. It criticizes the existing patchwork of privacy statutes as weak, incomplete, and fractured, and argue that it fails to provide across-the-board procedures empowering individuals to control the use of their personal information. Moreover, they decry the lack of clear guidance, oversight and enforcement, in the absence of an agency dedicated to data protection. And, while they differ in detail, academic and advocate proposals for reform generally concur that the increased focus of corporate attention and resources on privacy for which Smith called requires the model of protection adopted throughout Europe: omnibus FIPPS-based privacy principles in law or binding codes interpreted and monitored by an independent privacy agency.

This dominant critique of privacy requirements "on the books," however, has largely failed to take account of a sea change in corporate practices "on the ground"—and thus ignored a curious paradox for normative assessment.

Between 1995 and 2010, corporate privacy management in the U.S. has undergone a profound transformation. Following the lead of the financial and health sectors, thousands of companies have created Chief Privacy Officer positions, a development often accompanied by prominent publicity campaigns. A professional association of privacy professionals boasts over 6,500 members, and offers information-privacy training and certification. A robust privacy law practice has arisen to service the growing group of professionals and assist them in assessing and managing privacy. Pricewaterhouse Coopers and others conduct privacy audits across multiple sectors. And robust privacy seal and certification programs have developed.

Hence the paradox. In contrast to the lack of managerial "time and attention" devoted to privacy concerns documented fifteen years ago, corporate practice has promoted direct privacy leadership, in many instances by c-level executives managing large and well-resourced staffs. Yet these changes cannot be attributed to the prescription born of the dominant critique. U.S. privacy regulation remains fragmented and ambiguous, having failed to shed its siloed and sectoral emphasis. It has largely eschewed a commitment to robust FIPPS principles. Congress has declined to follow the European model; the U.S. still has no dedicated privacy administrator.

---

[9] *See id.* at 207-224.

[10] *See id.* at 210-11.

This paper, presenting the initial findings of the first empirical research into corporate privacy practices in fifteen years, seeks to address this paradox. This paper draws on semistructured qualitative interviews with Chief Privacy Officers identified as industry leaders by their peers, government officials, and journalists, to consider the following: If corporate attention to privacy seems to have flourished despite the failure to achieve what many believed were policy prerequisites, what has prompted the change? What was the role played by law, as opposed to other forces? And how do firms understand the meaning of privacy, despite external prompts that might seem as, or more, ambiguous as those identified by Jeff Smith fifteen years ago?

As described in Section II, although the leading CPOs we interviewed were at heterogeneous firms, they nonetheless communicated a coherent account in responding to these inquiries.

First, they consistently identified a profound shift in the definition of privacy, and its treatment. Each of the corporate privacy leaders defined information privacy as more than "information self-determination," protected by formal notice and consent, introducing as well a substantive notion of privacy rooted in *consumer expectations*. They understood the meaning of "privacy" to depend on the beliefs and assumptions of consumers as to the appropriate treatment of individual information and personal identity. These expectations, they indicated, evolve constantly, and change by context. The success of privacy protection, then, would be measured not by the vindication of notice and consent rights, but in the actual prevention of substantive harms, such as preventing data breaches, or treating information in a way that violates the "trust" of those whose information was at stake. The identification of privacy with consumer expectations as reflected in malleable context-dependent norms, moreover, has moved privacy from a compliance-oriented activity to a risk-assessment process, requiring firms to embed privacy in decisions about product design and market entry, as well as policy development.

Second, the interviews uniformly pointed to the importance of law in this definitional shift. While individual sectoral statutes might be responsible for firms' initial commitment of resources for privacy personnel, the path these professionals would take was influenced by two other regulatory developments. Most notable was the development of the Federal Trade Commission's role (as well as that of the state Attorneys General) as an "activist privacy regulator." Using its broad consumer protection authority, including the ability to shape the law through the threat of enforcement actions, the FTC has advanced an evolving consumer-oriented understanding of privacy. Additionally, the CPOs interviewed pointed to the passage of state security breach notification (SBN) laws as a means for binding corporate performance on privacy to reputation capital. This, they report, has had a significant effect on how privacy is perceived in the upper echelons of corporations, and accorded CPOs greater leverage to implement measures conforming with their notions of privacy within corporations. Taken together, these factors move corporations away from the reactive management style identified by Smith and away from a purely compliance-driven approach.

Finally, the interviews indicated a variety of non-legal phenomena central to the formation and diffusion of the legal notion of privacy compliance as consumer-harm-prevention. They discussed the role of both technology changes and third-party advocates in making consumer privacy protection a market reputation issue. And they discussed the importance of the professionalization of privacy officers as a force for transmission of consumer-expectation notions of privacy, and related "best practices," between firms.

Prompted by these interviews, Section III offers a new account of U.S. privacy "on the ground." It documents the uniquely American way in which the largely-procedural and individual-focused language of privacy protection has been augmented with a substantive concern for preventing violations of consumers' expectations about the treatment of information about them. Taking seriously the our respondents' attribution of this understanding to FTC behavior and other related activity, this section documents an account of the way in which privacy has been "reframed" over the past fifteen years, and its implications for corporate practices. This account emphasizes how elements largely neglected in the dominant "on the books" narrative—the emergence of the Federal Trade Commission as a privacy regulator, the enactment of SBN laws, the increasing influence of privacy advocates, market and media pressures for privacy-protection, and the rise of privacy professionals—took part in reconstructing privacy norms in consumer terms, and participated in the diffusion and institutionalization of those norms.

This grounded account, as Section IV argues, has profound implications for debates about both privacy law's substance, and its form.

Specifically, this account casts into relief the incompleteness of a reliance on formal notice, consent and information alone to protect privacy norms as rapid technology changes reduce the power of individuals to isolate and identify the use of data that concerns them. It suggests the frailty of a procedural understanding of privacy protection in guiding corporate decisionmakers, *ex ante*, in making choices about the technologies they employ in products or processes. And it identifies a substantive language for declaring that corporations should not engage in certain types of practices regardless of the formal procedures they have used—a robust, if still emerging, language that has helped frame criticisms of recent privacy invasions by Google Buzz, Sears, and Sony. Indeed, the consumer-protection lens reflects approaches that theorists suggest best vindicate individual and societal interests: those emphasizing objective expectations over subjective formalism, dynamism in the face of technological advance, and application by context.

Moreover, the account of privacy on the ground should inform debates over regulatory form. While the dominant account argues for greater uniformity and specificity in privacy law, the account on the ground suggests the value of governing privacy through flexible principles. Where Smith saw ambiguity as a "bug," we see it as a "feature." Our account describes how a regulator's entrepreneurial deployment of a broad and imprecise legal mandate centered a robust multi-player discourse about privacy that has focused market pressure and executive resources. The increase in

corporate time and attention, accordingly, arose because, rather than in spite, of regulatory ambiguity.

Our research, as this Article's conclusion describes, redirects the unidemensional debate over the adequacy of U.S. information privacy law "on the books"—including arguments over whether U.S. law should mimic the EU model—just at the time that Congress, the Obama Administration, and international organizations are revisiting national and global approaches to privacy approaches. While bolstered procedural mechanisms for enhancing individual choices might be needed, pursuing that goal in a way that eclipses robust substantive protections, or constrains the regulatory flexibility that permits their evolution, will destroy important tools for overcoming corporate over-reaching, consumer manipulation, and the collective action problems raised by ceding privacy protection to individual choice alone.

I. THE DEBATE OVER U.S. PRIVACY POLICY ON THE BOOKS

The adequacy of U.S. information privacy law is the subject of heated debate. A majority of privacy scholars and advocates criticize existing regulation for its market-based and sectoral approach to privacy protection in the corporate sector, and contend that the existing patchwork of U.S. regulation fails to ensure across-the-board conformity with the standard measure of privacy protection: compliance with the Fair Information Practice Principles (FIPPS) first articulated in the early 1970s. Legal academics and privacy experts have labeled the U.S. approach "FIPPS-lite[11]," an unfavorable comparison to the European Union where FIPPS are reflected through omnibus laws designed to structure all facets of data processing in the private and public sector, and centralized data protection agencies established to enforce them. Thus, they argue for the passage of omnibus U.S. legislation protecting "informational self-determination"—and mandating specific procedures for giving individuals greater control over information about them.

These critiques' descriptive claims regarding the nature of U.S. law on the books are, we readily agree, generally accurate. U.S. privacy law, and its enforcement, are fragmented, and depart frequently from a "FIPPS" understanding of the meaning of privacy.

But their normative and predictive conclusions adopted by many scholars and advocates—that policymakers should act under the belief that U.S. firms will not adopt privacy-protective practices without the passage of across-the-board procedural requirements—have remained troublingly constant given the radical shifts in the landscape of U.S. privacy law. Focusing on a debate between legislative and market mechanisms to protect privacy, the dialogue about protecting privacy in the U.S. has often ignored changes in both the substantive definition of privacy and the mechanisms for its protection that have emerged in the U.S. since Jeff Smith's study, and the ways in

---

[11] Advocates Privacy-lite http://www.privacyrights.org/ar/Privacy-IssuesList.htm; http://judiciary.house.gov/Legacy/mierzwinski050102.htm

which those developments have shaped corporate practice. And they are worth reconsideration.

A. The Dominant Discourse

1. The Touchstone for Measurement: Comprehensive FIPPS-based Regulation and Enforcement

The foundation of information privacy protection throughout much of the world is "informational self-determination"[12] or "the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others."[13] This rights-based conception of information privacy is embodied a set of "Fair Information Privacy Practices" which provide the backbone of data protection laws in Europe and many other countries.

The Organization for Economic Cooperation and Development (OECD)'s *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, finalized three decades ago, provides an influential statement of FIPPS.[14] It articulates eight principles to "harmonise national privacy legislation, while upholding such human rights . . . at the same time prevent interruptions in international flows of data."[15] These principles emphasize an individual's knowledge, participation and control over personal information. They embrace transparency about the types of information collected and the way the information will be used. They propose certain limits on data collection—namely that "data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[16] They require data collectors to maintain information securely, and emphasize the rights of data subjects to access, and ensure the accuracy of, personal information.[17] And they link the use and disclosure of information to principles of individual self-determination. Thus a FIPPS approach relies largely on procedural protections, such as providing notice to the "data subject," as well as notions of "consent" to informational use.

A full implementation of the FIPPS approach's conception of data protection as a means of protecting individual rights is reflected in comprehensive laws governing information collection and use regardless of type and sector. Moreover, privacy scholars

---

[12] The term "information self-determination" was set forth in a German court decision limiting the intrusiveness of the census. See Judgment of the First Senate [Bverfge, Karlsruhe],, Dec. 15, 1983], translated in 5 HUM. RTS. L. J. 94 (1984).

[13] Alan F. Westin, Privacy and Freedom (New York: Atheneum Press, 1967) p. 7.

[14] O.E.C.D. Doc. C 58 (final) (Oct. 1, 1980); *see* Colin Bennett, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 101-111 (1992) (describing the OECD principles).

[15] O.E.C.D. Doc. C 58 (final) (Oct. 1, 1980).

[16] *Id.* (Guideline 1).

[17] Many FIPPS proponents consider such access rights to be "the most important privacy protection safeguard." BENNETT, *supra* note _, at 103.

committed to such a rights-based conception of information privacy protection have emphasized the importance of a strong single privacy enforcement authority that "knows exactly when to use the carrot and when to use the stick, and who is not concerned with balancing data protection with other administrative and political values."[18]

These elements of privacy governance—comprehensive, procedural protections enforced uniformly by a dedicated privacy agency—typify the European approach. And they have served as the dominant metric against which the adequacy of U.S. regulation has been assessed in the policy debate.

2. The Prevailing Critique of U.S. Privacy Statutes

In measuring the U.S. privacy framework against the metric of the European data protection approach, critics have found the former sorely lacking on all three dimensions.[19] "In contrast to the approach in many other nations," one scholar summarizes, "it is unusual in the United States to find any comprehensive privacy laws, which legal experts term 'omnibus laws' and that enumerate a complete set of rights and responsibilities for those who process personal data."[20] Rather, "regulation of the treatment of personal information in the United States occurs through attention to discrete areas of information use" targeting "specific, sectoral activities, such as credit reporting," health care, or electronic commerce.[21] Accordingly, informational privacy is governed by a variety of different laws, administered by different agencies—or sometimes by no agency at all[22]—setting forth divergent requirements governing the treatment of information by type, and business sector.[23]

---

[18] Bennett, *supra* note _, at 239 (describing the arguments of David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States (1989).

[19] See Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime Of Privacy Protection*, 2006 U. ILL. L. REV. 357, 358 (2006) ("Privacy protection in the United States has often been criticized."); Ira S. Rubinstein, *Privacy, Self-Regulation and Statutory Safe Harbors, available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1510275 ("According to its many critics, privacy self-regulation is a failure. It suffers from weak or incomplete realization of Fair Information Practice Principles, inadequate incentives to ensure wide scale industry participation, ineffective compliance and enforcement mechanisms, and an overall lack of transparency.")

[20] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1932 (1999).

[21] *Id.*

[22] *See*, *e.g.*, Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510 (extending restrictions against wiretaps to include transmissions of electronic data by computer); Video Privacy Protection Act of 1988 (VPPA), 18 U.S.C. § 2710 (preventing disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual material"); Right to Financial Privacy Act (RFPA), 12 U.S.C. §§ 3401-342 (protecting the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records).

[23] *See*, *e.g.*, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No.

The formal regulations that result provide uneven protection for personal information, and unequal treatment even for similarly situated industry players. Privacy protections, for example, often turn on the entity collecting personal information. Doctors and pharmacies are clearly covered by both federal and state privacy statutes protecting health information,[24] while the developing "personal health portals" designed to create portable "patient-controlled" health records may fall completely outside the scope of such laws, depending upon their business models. Similarly, privacy protection for information about an individual's location generated through the use of location enabled services, a mapping service used on a personal digital assistant (PDA) such as an iPhone or Treo, or a car-based service such as GM Onstar, will vary depending upon whether or not it is provided by a "telecommunications carrier" who is covered by specific regulations, or by another type of service or application provider.

The policies animating different U.S. privacy statutes, moreover, vary considerably. Early privacy statutes, notably the Fair Credit Reporting Act of 1970 (FCRA),[25] which regulates credit reporting activities, and the Privacy Act of 1974,[26] which regulates collection and use of data by government agencies, reflect FIPPS' "informational-self determination" rubric, and include a full range of safeguards reflecting those principles' emphasis on notice, information, and consent.[27] Yet more recent privacy measures often stem not from a commitment to informational-self determination, but from more instrumental concerns arising from harms experienced by consumers, or perceived threats to other interests. Such concerns highlight privacy as a means of promoting social goals like the efficacy of doctor-patient relationship, or of commercial exchanges—the notion, for example, that "privacy laws might promote confidence in Internet commerce, with benefits both for surfers' privacy and companies' sales."[28] Such instrumental approaches, and the balance between privacy and other values they implicate, were reflected in formative decisions regarding the governance of

---

104-191, 110 Stat. 1936 (1996) (regulating the use and disclosure of "Protected Health Information"); Title V of Gramm–Leach–Bliley Act (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801–6827 (2006)), 15 U.S.C. §§ 6801, 6805 (empowering various agencies to promulgate data-security regulations for financial institutions).

[24] HIPAA's Privacy Rule, for example, regulates only the use and disclosure of certain information held by "covered entities." generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions, 45 C.F.R. 164.501.

[25] 15 U.S.C. § 1681.

[26] 5 U.S.C. § 552a.

[27] *See* Solove & Hoofnagle, *supra* note __, 359-361 (discussing those two laws); *see also id*. at 357 (explaining how "emerging companies known as 'commercial data brokers' have frequently slipped through the cracks" these laws).

[28] Peter P. Swire, Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy, 54 HASTINGS L. J. 847, 861-862 (2003).

privacy on the Internet, which was characterized by limited government mandates supplemented by significant reliance on "self-regulation" by industry players.[29]

These elements of U.S privacy regulation have left it ripe for critique. First, scholars, advocates, and politicians alike charge that the "patchwork,"[30] nature of U.S. privacy statutes renders them underinclusive in its coverage of data worthy of protection, makes arbitrary distinctions that create confusion among both those who are regulated and those who are intended to enjoy protection, and provides only static protections, unable to evolve as technologies and business practices change.[31] Thus in many realms, privacy is protected only by self-regulation by market actors themselves, which is bound to fail in the absence of external incentives for information protection. [32]

---

[29] *See*, *e.g.*, WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997) (promoting self-regulation as the preferred approach to protecting online privacy); Rubinstein, *supra* note _ at 5 ("Clinton officials generally favored the view that private sector leadership would cause electronic commerce to flourish, and specifically supported efforts to implement meaningful, consumer-friendly, self-regulatory privacy regimes in combination with technology solutions.")

[30] Center for Democracy & Technology, *Webpage*, "Consumer Privacy" ("While privacy faces threats from both private and government intrusions, the existing motley patchwork of privacy laws and practices fails to provide comprehensive protection. Instead, it causes confusion that fuels a sense of distrust and skepticism, limiting realization of the Internet's potential."); Beth Givens, Privacy Rights Clearinghouse, *Financial Privacy: The Shortcomings of the Federal Financial Services Modernization Act* (September 15, 2000) ("Our approach is characterized as a 'patchwork' of laws.); Priscilla M. Regan, Safe Harbors or Free Frontiers? *Privacy and Transborder Data Flows*, 59 J. SOC. ISSUES 263, 266 (2003) (discussing "[t]he patchwork of sectoral regulation that has long confused the Europeans"); Larry Dignan, *Senate, Web Ad Titans Joust Over Behavioral Targeting*, Between the Lines Blog (posted July 9, 2008), available at http://blogs.zdnet.com/BTL/?p=9280 (quoting U.S. Senator Daniel K. Inouye as saying that "I fear that our existing patchwork of sector-specific privacy laws provides American consumers with virtually no protection.").

[31] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 48 (2001) ("The coverage of U.S. law was uneven: Fair Information Practices were in force in some sectors and not others. There was inadequate enforcement and oversight. Technology continued to outpace the law. And the failure to adopt a comprehensive legal framework to safeguard privacy rights could jeopardize transborder data flows with Europe and other regions.")

[32] Chris Jay Hoofnagle, Electronic Privacy Information Center, *Privacy Self-Regulation: A Decade of Disappointment*, (March 4, 2005), *available at* http://epic.org/reports/decadedisappoint.pdf ("[T]en years of self regulation has led to serious failures in this field. The online privacy situation is getting worse, so bad that offline retailers are emulating the worst Internet practices . . . the market has been a driving force in eroding both practices and expectations."); Joel Reidenberg, "Restoring Americans' Privacy in Electronic Commerce," 14 BERKELEY TECH. L.J. 771 (1999) (responding in part to WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (July 1, 1997), critiquing U.S. reliance on self regulation, and proposing FIPPS-based regulation).

Second, critics reject protections that do exist as "FIPPS-lite,"[33] failing to embody the robust procedures embraced by Fair Information Principles.[34] They contend, moreover that the turn to market-oriented rationales for privacy protection diminish the moral weight of privacy—reducing it to another item to be bartered and traded on the market—and fails to recognize the relationship between privacy and democratic society.[35]

Finally, they argue that the failure of the U.S. to centralize oversight of privacy in a single agency able to provide guidance to industry, evolve privacy rules to address emerging issues, and advocate for privacy protection across the public and private sector.[36]

These criticisms, and the metric they use, have dominated the policy debate. Scholars and advocates have been joined by industry leaders and politicians in support of passage of omnibus legislation requiring the adoption of FIPPS generally, sometimes coupled with the creation of an independent agency to oversee and enforce implementation.[37] Thus much of the dominant debate involves a normative claim that the current approach (in particular as measured by the EU data protection model) has failed to provide meaningful corporate privacy practices, and must be replaced by an "enforcement model of regulation (which is also referred to as command-and-control regulation)," in which "Congress defines a set of privacy rules for commercial firms based on FIPPS and authorizes agency regulation, which is then supplemented over time by court decisions interpreting the rules."[38]

B. Reevaluating the Dominant Debate—Indications from Privacy on the Ground

As a descriptive matter, the dominant critiques present a largely accurate picture of statutes and regulations governing U.S. privacy law on the books. Statutes provide

---

[33] Edmund Mierzwinski, Testimony of the U.S. Public Interest Research Group Concerning Affiliate Sharing Practices and the Fair Credit Reporting Act Before the Senate Banking Committee (June 26, 2003) (criticizing the Gramm-Leach-Bliley Act's provisions regarding treatment of personal financial information as "at best, based on FIPPS-Lite").

[34] Solove & Hoofnagle, *supra* note _ at 358 ("Privacy experts have long suggested that information collection be consistent with Fair Information Practices.").

[35] See Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553 (1995); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707 (1987).

[36] *See* sources cited in *supra*, note _.

[37] See, *Consumer Privacy Legislative Forum Statement of Support in Principle for Comprehensive Consumer Privacy Legislation*, June 20, 2006 (signatories Eastman Kodak Co., eBay Inc., Eli Lilly and Co., Google, Inc., Hewitt and Associates, Hewlett-Packard Co., Intel Corp., Microsoft Corp., Oracle Corp., Procter & Gamble Co., Sun Microsystems, Inc., Symantec Corp.).

[38] Rubinstein, *supra* note _ at 2.

inconsistent treatment of similar information and similar business activities leading to an uneven playing field for business and an unpredictable set of protections for individuals. Historically the absence of leadership and coordination on privacy has resulted in inconsistent adherence to existing law and a generally reactive stance to privacy within and by federal agencies. Finally promoting consumer trust, rather than protecting individual privacy, motivates many recent privacy interventions.

As accurate as this debate over the approach to privacy *on the books* may be, it gives short shrift—and therefore provides limited insight into—the ways in which individual privacy is protected "*on the ground*," by both regulators and corporate actors. This cursory treatment was unfortunate but understandable given the relative paucity of attention to privacy in the U.S. commercial sector between formulation of FIPPS as the crux of data protection in the 1970s and the mid-1990s. However, it bespeaks an inexplicable lack of engagement with the U.S. privacy framework that has emerged over the last ten years. In some ways, it therefore puts the cart before the horse, by proceeding to prescriptions about how to improve privacy protection without taking stock of the privacy practices in place within corporations, and how regulatory changes might affect those practices, for better or worse.

This Article begins from the position that the debate about how to move forward on privacy would benefit from a description of the working definition of privacy adopted by corporations, how that definition drives corporate practice on the ground, and how it is influenced by actual regulatory practice.

Since Smith's 1994 study, we have little information about how changes in the U.S. privacy framework—including the panoply of obligations on U.S. companies introduced incrementally by Congress, the FTC and state Attorneys Generals, and changes in the institutional structure of privacy oversight such as the increasing array of individuals in the public and private sector specifically tasked with protecting privacy and the growth of informal and formal tools developed to assist them in this work—have affected corporate practice.

Yet if the critiques of U.S. privacy law demonstrate constancy, corporate privacy practices on the ground evidence a sea change. In the nearly fifteen years since Smith's indictment regarding the lack of "time and attention" devoted to privacy by corporate managers, external signs of a shift in corporate privacy management abound. Smith determined that corporate privacy was mired in a cycle of ongoing policy drift, received only episodic and reactive attention from upper level managers; and was comprised of "non-existent policies in important areas and a persistent policy/practice gap." Yet today, corporate structures frequently include direct privacy leadership, in many instances by c-level executives. The individuals managing corporate privacy have an applicant pool of trained professionals to draw from. There is ongoing training, certification, and networking. A community of corporate privacy managers has emerged. Ready evidence suggests that substantial effort is made to manage privacy.

1. Indications of a Sea Change: The Rise of the Chief Privacy Officer

The development of the corporate Chief Privacy Officer offers the most ready evidence of sea change in privacy management In the late 1990's, companies in the financial and health sectors began creating chief privacy officer positions.[39] By 2000, companies in other sectors created CPO positions as well[40]—often to great fanfare, as evidenced by numerous press releases announcing the appointments.[41] Companies' motivations for creating CPO positions were glibly summarized by Richard Purcell, Microsoft's Chief Privacy Officer, in remarks at a large security conference, "How do we get to that vocabulary, that purpose and that channel of communication," he asked, "that assures consumers that we aren't a lot of evil-headed monsters?"[42]

With somewhat amazing alacrity, the informational, training and networking needs of these newly appointed CPOs was met by a new trade association, the Association of Corporate Privacy Officers. Formed in 2001 by Alan Westin, the association—which later developed into the "International Association of Privacy Professionals" (IAPP)—quickly went about formalizing educational programs and undertaking studies to understand the needs and activities of this new profession.[43] About the same time, the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA5) created a Privacy Task Force that eventually developed the Generally Accepted Privacy Principles (GAPP), which provide the basis for privacy audits. Privacy seal and certification programs originated during this time as well. TRUSTe, the first online privacy seal program was founded in 1997 and currently has seals at 3,440 web sites. The Better Business Bureau

---

[39] Christopher Brown, *Survey Finds Increasing Number of Firms Appointing Officers with institutional Clout*, 1 PRIV. & SECURITY LAW REPT. 78 (Jan. 28, 2002). It appears that first US privacy officer was Jennifer Barrett of Acxiom, an information services company. Barrett joined the company in 1974, working in many departments of Acxiom, and became a vice president of the company in 1981. Since 1991, she has been responsible for managing privacy issues at Acxiom. ACXIOM CORPORATE LEADERSHIP, available at http://www.acxiom.com/default.aspx?ID=1667&DisplayID=18.

[40] For example, Ray Everett-Church (who claims to be the first CPO) was appointed to such a position by AllAdvantage.com in 2000. Ray Everett-Church, available at http://www.everett.org/about.shtml.

[41] *See, e.g.*, Linda Rosencrance, *IBM Joins Chief Privacy Officer Trend*, Computerworld, Nov. 30, 2000, available at http://www.computerworld.com.au/index.php?id=574929492 (announcing IBM's appointment of Harriet Pearson to a newly created executive-level CPO position); Earthlink, *Earthlink Names Chief Privacy Officer*, available at http://www.earthlink.net/about/press/pr_cpo_announce/ (announcing the appointment of Les Seagraves as CPO); Yukika Awazua and Kevin C. Desouzab, "The Knowledge Chiefs: CKOs, CLOs and CPOs," EUROP. MANAG. J. Vol. 22, No. 3, pp. 339–344, 341 2004 (CPO positions publicly announced on PR Wire and Business Wire covered financial services, banking and insurance (8), marketing and advertising(7), Healthcare (6), Computer Hardware (3), Computer Software (5), Communication Services (4), Consulting (4), and other (including information services and consumer electronics) (3)).

[42] John Schwartz, *Conference Seeks to Balance Web Security and Privacy*, N.Y. TIMES, Dec. 8, 2000, at C4.

[43] Email from the Center for Social & Legal Research to subscribers, P&AB/CSLR Closing, Sept. 14, 2006 (on file with authors).

launched a privacy seal program shortly thereafter and its Children's Advertising Review Unit is the primary self-regulatory program for web sites directed at children.

By 2002, the number of corporate CPOs had reached 500, while in 2003, the IAPP claimed 1000 overall members.[44] In 2004, the association debuted a certification program in corporate privacy compliance, which certified 350 professionals within a year.[45] And today, the IAPP boasts 6,000 members from businesses, governments and academic institutions across 47 countries.[46] IAPP runs a credentialing program in information privacy, the Certified Information Privacy Professional (CIPP) and provides educational materials and runs a wide range of educational and professional conference.[47]

Survey data, moreover, shows that Chief Privacy Officers (CPOs) continue to become more common, and more powerful, features within corporate structures. Within many Fortune 500 companies CPOs are directors or c-level executives,[48] evidencing a perception of privacy as a strategic matter. And corporate privacy resources expand outside firm structures as well. Pricewaterhouse Coopers and others conduct privacy audits across multiple sectors. A robust privacy law practice has arisen to service "in house" professionals and assist them in assessing and managing privacy. Several self-regulatory organizations provide oversight and enforcement of voluntarily adopted privacy policies, advice and support to businesses on privacy issues, handle consumer complaints and monitor members' privacy commitments.[49]

One additional measure, qualitative but perhaps more substantive, of the changes in corporate privacy management deserves mention here. In 1995, Smith referred to his study as the "study that almost wasn't."[50] He details the difficulties he faced in securing institutional participation. Despite his faculty position at a leading business school, strong entrée to high-level executives made possible through faculty and colleagues with existing institutional contacts, and iron-clad promises of anonymity, Smith experienced repeated rejections. Many of the rejections followed an initial positive response, and appeared to be driven by corporate lawyers and a overall sense that the topic of privacy was too sensitive and volatile to discuss publicly.[51] Furthermore, while Smith eventually secured seven participants, even they remained

---

[44] Privacy Officers Association Changes Name, 2 Priv. & Security L. Rept. 39 (Jan. 13, 2003).

[45] http://www.marketwire.com/press-release/Iapp-735905.html.

[46] https://www.privacyassociation.org/index.php.

[47] https://www.privacyassociation.org/index.php?option=com_content&task=view&id=2&Itemid=148 .

[48] *See* Ponemon Institute, *Privacy Professional's Role, Function and Salary Survey* (2005) ("50 percent of privacy professionals are at a director or higher level within their firms; 84 percent report their position is a full-time role within their organization; 42 percent said their department has a direct line of report to a C-level executive within the organization, while 25 percent have a direct line of report to General Counsel");.

[49] Truste, Better Business Bureau Program Privacy Seal, Children's Advertising Reivew Unit

[50] SMITH, *supra* note __, at 52.

[51] *Id.* at 54.

uneasy about such scrutiny. For example, Smith quotes one executive as saying, "I feel somewhat like we are standing nude before you . . . . It will probably be a healthy experience for us to see ourselves thorough the eyes of an outsider, but I imagine it will ultimately be painful."[52]

By contrast, the high-level corporate officials we contacted for the study discussed below were willing, and some quite eager, to participate in the study, to see our findings and conclusions, and to share them with others. While top news headlines affirm that privacy remains a high-profile, hot button topic, the companies we contacted welcomed the chance to share information about how they handle personal information. The marked change in corporate response to similar requests to participate in studies of corporate privacy management are, we believe, a strong indication that privacy is out of the closet and has become a topic corporate executives are willing to discuss candidly.

Taking seriously these external indicia of a massive increase in privacy resources, the remainder of the Article digs deeper. Rooted in qualitative research into corporate privacy management, it presents a new account of "privacy on the ground," an account which should inform, and transform, the policy debate moving forward.

II. INVESTIGATING PRIVACY ON THE GROUND- EMPIRICAL EVIDENCE FROM CPO INTERVIEWS

To that end, we have embarked on a wide-ranging project to collect empirical information—both qualitative and quantitative—documenting privacy's operationalization "on the ground."[53] The earliest evidence from this project—derived from semi-structured qualitative interviews with nine Chief Privacy Officers identified as field leaders, is presented below. This subset of privacy professionals was identified by domain experts—leading privacy thinkers (both lawyers and non-lawyers) drawn from academia, legal practice (in house and firms), trade groups, advocacy groups, a consultancy, a federal government agency, and journalists focusing on privacy issues—using a snowball-sampling technique.

The structure and purpose of the interviews, sought to minimize the effects of the bias inherent in these selection methods. Snowball samples tends to include participants with thick social networks in a field, and our sample focused on domain leaders with interests in the way discussions of privacy were constructed. The interviews accordingly sought to capture the way in which players with these very characteristics—those "key informants" at the center of the privacy field—framed the privacy discourse. This framing, in turn, is contextualized in Section III, by explication of the privacy regulation and advocacy discourse more broadly.

---

[52] SMITH, *supra* note __, at 54.

[53] Other elements of this empirical project include parallel interviews of European Chief Privacy Officers, surveys of U.S. and European privacy officers more generally, and comparative empirical assessments of enforcement techniques.

The privacy leaders interviewed came from firms that were heterogeneous on every metric except size—all but one was a Fortune 1000 company. The firms hailed both from industries governed by sector-specific privacy statutes, and from unregulated sectors. Some claim global presence; others' only domestic scope. Some include highly diversified business lines, while others are focused within a single industry sector. Many focused on technology-intensive products and services, while others engaged in more traditional lines of business. Moreover, those interviewed had varied personal characteristics. Some were lawyers, others had operational or technical expertise. Some worked under the auspices of the corporate legal department; others as free-standing officers. A number had worked in government, while most had exclusively private-sector careers.

Yet despite this diversity, the interviewees conveyed a high degree of coherence regarding the constellation of issues about which we asked—the way privacy is defined and its protection is operationalized within corporations, as well as the extra- and intra-firm forces that shape these understandings. Specifically, they presented important consistency as to (1) the relevance of a legal "compliance" approach—FIPPS or otherwise—to corporate privacy practices; (2) the way in which privacy concerns are framed and measured within corporations; and (3) the role of external forces—specifically law, markets, advocates and professions—in shaping that framing.

A. The Limited Import of the "Rules-Compliance" approach to Privacy

In response to open-ended questions about the "external factors" shaping their corporations' privacy practices, respondents articulated a consistent view of the role of compliance with specific legal requirements—both those arising from the EU and those originating in the U.S. sectoral-based regime. By their description, specific legal rules were important in shaping certain "compliance-oriented" measures but played only a limited role in animating corporate policy and principles more broadly.

1. The Role of Legal Rules

Thus, when asked about the external or environmental forces that shaped particular practices in their firms, each respondent identified particular U.S. sectoral statutes, and, for those conducting business abroad, the E.U. Privacy Directive. They pointed, however, to the limited role of legal compliance with codified requirements played in constituting their understanding of what "privacy" demanded of corporate actors.

"[O]bviously," stated one respondent, specific "statutes and regulations" shape particular privacy practices.[54] In the words of others, they constitute the "starting point," "the backing" of an approach to privacy, or the "bottom" of the "privacy triangle."

---

[54] To protect respondent confidentiality, we have removed the interview citations, which are on file with the authors, from the version of this draft submitted to law reviews. Before publication, we will work with Law Review editors to develop a citation system that conforms to privacy practices.

Thus central to the attention accorded privacy is the reality that "[p]rivacy has parts of that, which is you have to comply with some of these laws that are out there." Compliance, then, "has driven the issue to some extent," in that companies must "always meet the legal compliance."

Moreover, several cited compliance with high-profile, and highly-specified, regulatory regimes as a means for signaling privacy leadership to consumers, businesses, and foreign regulators. As to the first, one respondent explained,

> I think that there is some benefit . . . from the consumer perspective, even though they don't understand HIPAA, to know that there is some federal law that makes it criminal if they misuse data. . . . [O]ne thing I think that HIPAA does well is it helps, in whatever fashion, tell the consumer, look, you're protected in this sphere. I don't think they understand it but I think it helps.

Compliance with the Department of Commerce-negotiated "Safe Harbor" certification of corporate conformity with EU privacy law[55] plays a similar signaling function for business partners, explained a different respondent in the business-to-business sector. Discussing his firm's choice between attaining Safe Harbor certification and instead enforcing privacy safeguards through contracts with outsourcers, he described:

> Well for instance, whether we decided to go for Safe Harbor or for contracts was really driven to a large extent by customers who started asking us, "Are you members of the Safe Harbor?" So we actually had a customer push because, for them, it was a checkbox, and the contract for them was much harder to manage than saying, I'm dealing with a Safe Harbor company so I have an adequacy. So we had a customer push and that helped us make the decision, because we were kind of on the fence.

2. The Shortcomings of Rules for Privacy Decisionmaking

Yet at the same time, every respondent—whether in highly regulated industries or those less burdened by sectoral regulation—spoke about the limited role that specific legal rules played in directly shaping their actual understanding of privacy's meaning. Those mandates, remarked one CPO, "enforce the minimum;" another continued: "then we build from there."

More respondents emphasized that specific procedural rules lack relevance to many privacy-impacting decisions that must be made by corporate managers. Specifically, they described the failure of such rules to offer a touchstone for guiding privacy decisionmaking in new contexts, as new types of products, technologies and business models evolve. As the boundaries between firms and the consumers and businesses with which they deal blur, and part of the value of products and services arises specifically from the purposeful sharing of information between business and consumer, the privacy threat model shifts from issues of "security," "access," "notice" and "consent"—dominant in U.S. FIPPS discourse—to questions of the reuse and

[55] *See infra* text at nn.__-__.

repurposing of information, and what notice and consent mean when companies can, while still in formal compliance with the law, manipulate huge amounts of data willingly supplied to them by consumers.

While each respondent spoke about potential privacy issues arising out of evolving product or service offerings or innovative organizational structures in the contexts of their particular firms, several examples illustrate the shortcomings of such static laws in providing a helpful guide in dynamic business contexts.

The most wide-reaching example arises from the societal shift towards "ubiquitous computing."[56] As companies root consumer or customer interactions in increased connectivity—ongoing relationships in place of one-off transactions—the use and transfer of data is constant. Indeed, respondents explained that the very fact of a communication itself may reflect information revealing that a recipient falls in a certain category: that they are an account holder, or use particular information products or services, or that they have a disease and are involved in ongoing medical treatment, , or are in a specific location—with all that might reveal. Data flows coming in and out of a home on a "smart" energy grid—data that may be readily shared for the purpose of enabling energy management—is an example of an environment that might also reveal significant information the activities on the inhabitant.[57] Moreover, explained another, previously nonproblemmatic policies such as monitoring communication to audit the quality of customer service take on new meaning, as personal information is revealed to third parties uninvolved with the service provision itself. In each case a customer might have been made aware of the privacy practices consistent with FIPPS policies, and the firm involved might have complied with all legal requirements, yet reasonable concerns about the integrity of privacy protections might nonetheless be triggered. In such new and changing contexts these regulatory approaches to privacy frequently fail to provide a metric for arriving at the appropriate balance between "value information flows and being technology-enabled" on the one hand, and "privacy-centric" or "trust-generating" concerns on the other.

Indeed, many new business services explicitly involve open-ended and ongoing corporate use and reuse of information in ways that develop over time. These services focus on the continuing manipulation of data to provide a "value proposition" to the "person who is giving us the information so they see some value coming back."

One sector operating in this manner identified by a number of respondents was healthcare, in which those other than traditional medical providers—such as pharmaceutical companies and medical technology firms—play an increasing role in ongoing oversight and monitoring of health practices and outcomes. Thus one

---

[56] Ubiquitous computing environments are those in "which each person is continually interacting with hundreds of nearby wirelessly interconnected computers. The point is to achieve the most effective kind of technology, that which is essentially invisible to the user," *See* M. Weiser, *Some Computer Science Issues in Ubiquitous Computing*, 36 ACM 75 (1993).

[57] *See* Mikhail A. Lisovich & Deirdre K. Mulligan, *Inferring Personal Information from Demand-Response Systems*, 8 IEEE Security and Privacy 11-20 (2010).

respondent described these shifts in their own company which now both "provid[es] IT systems for hospitals," and "make[s] all sorts of machines that you would see in a hospital" such as "diagnostic and interventional medical devices" that "go into the body." While these lines of business certainly require "thinking about HIPAA," they require deeper assessments ungoverned by either rights-based or process/access notions of privacy: "when you obviously get into the body," this respondent noted, "you've got all sorts of different healthcare privacy issues."

Another privacy officer spoke about the challenge of personalizing medicine, as research has demonstrated that there are "different tumor types," "different types of diabetics" and the fact that patients have "different kinds of diseases so they need different types of interventions." "[A]s you start to personalize," the respondent noted, "this requires more interaction with consumers." Moreover,

> we may need to try and figure out how to work or partner with another entity that has a tissue bank or we may need to figure out how to get access to a significant database that will allow our research to go forward. And the figuring out has to take into consideration, you know, what are the ethics? You know, what are the privacy issues around doing that?

While consumers, fully informed about the privacy practices and legal compliance regime governing the relevant company, might be truly interested in reaping the value resulting from the exchange of sensitive personal information, these trends, another CPO explained, reflect "fits and starts in the healthcare industry about its adoption of IT and the true connection of the different elements of that ecosystem," that raise potential new privacy issues.

Respondents thus identified the shortcomings of a "compliance-based" approach in a variety of contexts where technology supports the growing business trend towards ongoing remote communications with a product or service provider. Such technologies include, for example, means for remote transmission of data and information regarding software updates, and sensor technologies that convey usage and performance information back to manufacturers—information that consumers would, for some purposes, very much want corporations to have. In discussing this issue, one respondent noted their commitment to FIPPS: "We are an informed consent company. That's been my mantra. Informed consent is something a hundred years old. We can draw our little common-law hooks around it." Yet, she noted, this is an area in which FIPPS's rights-based notion of privacy fails to provide guidance:

> Opt in and opt out drives me crazy, especially when you talk about peripheral devices. How do you "opt in" to a [product] telling [the manufacturer] that it burned out? And do you want to? Probably not."

Finally, respondents spoke about the challenges arising from the potential privacy issues arising when two types of third parties—outsourcers and the government, under its subpoena power—are accorded, or seek, access to personal data. In both cases the original firm might justify sharing information by its compliance with governing legal rules; they can rely in the fact that they ensured that data transfers complied with the Safe Harbor or other regulatory requirements, or that they faced no legal obligation that

would hinder their release of data to a government agency. Yet both of these instances clearly implicate deeper privacy questions about the potential compromise of personal information—questions regarding which existing legal rules provide no answers.

Accordingly, respondents uniformly rejected an understanding of privacy as a compliance function. "[T]he law in privacy," one respondent summarized, "will only get you so far." Regarding many things that "privacy" requires, said another, "there's no law that says 'you have to do this.'" In sum, explained a third, broader principles have to be developed that can guide privacy decisions consistently in a variety of contexts—privacy must be "strategic, part of the technical strategy and the business strategy."

B. The Articulation of an Alternative Framing of Privacy

While our interviewees attributed a more "reactive" approach to specific legal rules governing privacy, they nonetheless described significant changes in the approach to corporate privacy since Smith's 1994 study. Specifically, they described the adoption of an approach to privacy issues in varying and dynamic contexts, wherever they arose in the firm—an approach, moreover, that was strikingly consistent across firms. This approach reflected an understanding that privacy is defined by consumer expectations regarding the appropriate treatment of personally-identifiable information. Such expectations evolved with changes in both technology, and consumers' methods of interaction with it, and therefore required the implementation of privacy practices that were dynamic and forward looking. This approach, moreover, stressed the importance of integrating practices into corporate decisionmaking that would prevent the violation of consumer expectations—a harm-avoidance approach—rather than any formal notion of informational self-determination rooted in formal notice or consent.

1. Company Law

For both operational and strategy reasons, then, respondents stressed the importance of developing "Company Law"—consistent and coordinated firm-specific global privacy policies intended to ensure that a firm is both in compliance with the requirements of all relevant jurisdictions, and at the same time acts concordantly when dealing with additional business issues not governed by any particular regulation.

Critically, these policies extend beyond compliance with specific legal mandates to broader privacy policies focused on outcomes: that, even if technically legal, corporate practices are "consistent with our global corporate values, and consistent with employing customer expectations."

2. Privacy Measured by "Consumer Expectations"

This last remark, identifying consumer expectations as a touchstone for developing corporate privacy practices, is reflected in every one of our respondents' description of their understanding as the "company" definition of privacy. Privacy, in respondents' language, has evolved over the last several years to be defined in large part by respect for what consumers expectat regarding the treatment of their personal sphere.

Such "customer or the individual expectations," guide behavior that exceeds the demands of legal compliance. In the words of one CPO, "your customers will hold you to a higher standard than laws will, and the question is, do you pay attention to your customers? Do you care about your customers?" The expectations approach was framed in relational terms, sounding in a normative language of "values," "ethical tone," "moral tone," and "integrity"; in experiential terms such as "secure, private, reliable,", and "consistent," and, most frequently, in fiduciary terms, such as "respect[ ]", " responsibility," stewardship, , and "protect[ion]." On a fundamental level, respondents repeated, privacy "equates to trust," "correlates to trust," is "a core value associated with trust," and, in the words of one: "Trust, trust, trust, trust."

Privacy leaders varied in their articulations of "consumer expectations," but sounded several consonant themes. Each emphasized the customer's experience, including "think[ing] about how this feels from the customer perspective, not what *we* think the customer needs to know." In so doing, one respondent described,

> you run it by your friends, you run it by your family; ask your mom, ask your granddad, ask somebody who doesn't live in this world or doesn't live in technology or the leading technology companies. What's the reaction? Do they laugh? That's one set of problems. Do they get the heebie jeebies, you know? Is it kind of creepy? So, the creepy factor, for lack of a better description is good.

Yet such expectations arise as well, they described, from the representations and actions of firms themselves: the "discrete behaviors that are going to be objectively put out there, subjectively put out there and then met," and the ability to "deliver those consistent experiences, compliant experiences, you know, that's trust."

Finally a consumer expectations approach was described with regards to outcomes, rather than particular rules or practices: "the end objective in my mind is always what's the right thing to do to maintain the company's trusted relationship with our employees, with our clients, with any constituency in society that has a relationship to us, which is probably pretty much any constituency." "[H]ow likely," for example, "is that customer going to be comfortable using online banking in the future or any other new online service that the bank offers, and how many friends is he likely to tell?" Or will "they start wanting to shut down the relationship, in other words shut off the information, complain to the FTC, send nasty letters and threatening lawsuits about email and that kind of stuff."

The fundamental implication of this definition of privacy, one respondent explained candidly, is that "it's not necessarily beginning from a privacy-as fundamental-right point of view," but rather reflects the notion of "privacy as important to what we do for a living."(VI:3)

3. Implications of a "Consumer Expectations" Framing: From Compliance to Risk Management

Defining privacy through a "consumer expectations" metric, the interviewees explained further, has important implications for both how firms need to think about

privacy protection, and, accordingly, how privacy protection is operationalized within the corporate structure.

The interviewed privacy officers sounded a consistent theme: that the definitional ambiguity inherent in privacy regulation required companies to embrace a dynamic, forward-looking outlook towards privacy. "[I]t's more than just statutory and regulatory," said one, "it's such an evolving area." "We're really defining [privacy as] 'Looking around corners . . . looking forward to things that are a few years out."

"We are all still learning," described another, "because the rules change:"

> Customer expectation changes and the employee expectations change. The world changes periodically too on top of that and I look at what we're doing as something that's really important from any kind of a personal and values perspective and from a business perspective.

In the words of a third: "[b]est in class is comparative, and it's also subjective. . . . [T]hat bar changes and it's different by industry and it's different by moment in time." A fourth echoed the contextual nature of the the "external environment" shaping privacy, including "how the regulations or even the perception of the public changes." Accordingly, explained a fifth, corporate leaders must focus on "What's the next thing that's coming down the pike, because if you get caught unawares, you're behind the ball and you're spending a lot of money."

This conceptualization of privacy issues, other respondents described, have shaped the way their companies have understood, and operationalized, the corporate privacy function. As rules-compliance provides an increasingly inapt mindset for privacy management, privacy is increasingly framed as part of the evolving practice of risk management. "[W]e're all talking about risk," said one interviewee, "And how do we mitigate risk at the same time we're . . . protecting information." Privacy, then, must be approached with the questions, "What do I need to be worrying about today? What am I missing?" Accordingly:

> I want to keep changing the way we're doing business so it is dynamic, so we are, you know, trying to mitigate the risk of the day while keeping our core program in place. And so we're changing . . . I don't keep [processes the same] the same. Because, if by chance it gets, you know, somebody figures a way to beat it, they won't be able to if I'm constantly changing it or adding something here or subtracting there. So my view is is it's a journey, not a destination, and we should always, we try to get everybody together to say, how do we mitigate risk; what's the latest, you know, what do we need to be-every time there is a breach I look at what happened and think, are we protected? So it's a constant, what's the next thing on the horizon?

Accordingly, as we discuss elsewhere,[58] privacy officers are incorporated into risk-management structures at the highest management level, and privacy discussions

---

[58] *See* Kenneth A. Bamberger and Deirdre K. Mulligan, *Operationalizing Privacy: Structures Within the Firm* (draft in progress).

have been moved out of compliance offices into the processes by which new products and services are developed.

C. External Influences on Privacy's Conception

Finally, respondents located the notion of privacy as a function of consumer expectations in particular developments over the last decade. As one respondent described, while a number of years ago "we talked to customers and said, 'How high on the radar is [privacy] for you?' And most of them at the beginning of this said, 'Not at all,'

> now we're seeing it pop up in RFPs in almost every selling instance. . . . And so these go on and on and that's something you never would have seen back in 2000, at least I never saw.

As another described,

> if you go back six, seven years ago, there was a change in the marketplace. Pre that time, no customer was demanding security in their solutions. They were demanding product features, and the more that you can ship me and the more that you can give me the capability to use, the better, and security just didn't matter at that point in time. I'm maybe going back just slightly pre seven years ago, but that changed with-- the market started to demand more security because security events started to become more common. And, we're a product company product companies produce what the market wants. The market doesn't want security, then you don't spend a lot of time thinking about security.(III)

This new emphasis on consumers and markets, they described, arose in the context of three intertwined phenomena central to development of a new privacy definition: (1) two regulatory developments—the Federal Trade Commission's expanded application of its consumer-protection enforcement authority pursuant to Section 5 of the FTC Act in the privacy context and the passage of state data breach notification statutes; (2) societal and technological changes that strengthened the role of advocates and the media; and (3) the professionalization of privacy officers.

1. Legal Developments

At the same time that respondents indicated the limited role of compliance with legal rules in shaping corporate approaches to privacy, every single respondent interviewed mentioned two important regulatory developments they believed central to shaping the current "consumer expectations" approach to privacy: the behavior of the FTC, and the enactment of state data breach notification statutes.

a. The Federal Trade Commission

Respondents uniformly pointed to the FTC's role as an "activist privacy regulator." in promoting the consumer protection understanding of privacy. As described below,[59] since 1996 the Federal Trade Commission has actively used its broad

[59] *See infra* Section III.

authority under Section 5 of the FTC Act, which prohibits "unfair or deceptive practices," to take an active role in the governance of privacy protection, ranging from issuing guidance regarding appropriate practices for protecting personal consumer information, to bringing enforcement actions challenging information practices alleged to cause consumer injury.

For three of the privacy leaders included in our study, the FTC's enforcement power held particular salience, as their firms had previously been subject to privacy enforcement actions by, or were currently governed by consent decrees with, the Commission. Yet respondents from firms uninvolved with previous FTC proceedings joined those three in referencing the threat of enforcement under the agency's broad authority as critical to the shaping of consumer-protection, rather than compliance-oriented, approaches to privacy. As an initial matter, they described, state-of-the-art privacy practices must reflect both "established real black letter law," and "FTC cases and best practices," including "all the enforcement actions [and] what the FTC is saying."

Perhaps more importantly, several respondents stressed, a key to the effectiveness of FTC enforcement authority is the agency's ability to respond to harmful outcomes by enforcing evolving standards of privacy protection as the market, technology, and consumer expectations change—the very opposite of the rule-based compliance approach frequently embodied by regulation. In acting against unfair and deceptive consumer practices, one respondent explained, the FTC has

> moved the bar over the last couple of years away from the sense that we're not exclusively focusing on deception and into the land of unfair. And in the land of unfair it's pretty foggy. The land of deception has become fairly clear over the years. There's always new situations that require an interpretation but there's some pretty clear rules of the road. I think the rules around unfair that we really have a fogged in set of landscaping here because unfair is much more subjective and the FTC has been pretty clear that they will figure out what it means at the time.

The unpredictability of future enforcement by the FTC and parallel state consumer protection officials contribute, others describe, to more forward-thinking and dynamic approaches to privacy policies in firms, guided by consumer-protection metric. One of those respondents in a firm subject to FTC oversight explained the ways in which the enforcement action against that company transformed the understanding of privacy in their, and other, firms, from one centered on compliance with *ex ante* rules to one animated by the avoidance of consumer harm. As that respondent explained, at the time of the privacy-compromising incident leading to the enforcement action,

> [W]e had everything in place, from a website security perspective, you know? We had, you know, SSL security, you know, in certain areas and in where we were collecting the information and we had, you know, a privacy statement that explained things . . . . [A]ll these things that we had in place that was fairly standard in corporate America at the time. I mean, we were consistent with the best practices at the time. I have no doubt about that. Our privacy policy was very standard for the time. (IV)

Yet the regulator determined that these "best practices" failed to conform with what should be expected of firms holding themselves out as privacy-protective:

> what we didn't have was the comprehensive program and the FTC, with our case, for the first time, looked at the privacy statement and said, "You know what? You can't say that you respect privacy and then not have a full privacy program with training." And now, you know, looking back, with six years of history, you say, well, yeah, okay, that's fairly fundamental. They've established that already. But even . . . when the incident occurred, you know, it was still pretty rare for companies to have the comprehensive program behind the website statement.
>
> * * *
>
> And so we did our walk around with the FTC commissioners, I went with my general counsel, and it was a completely eye opening thing for her. And there were exchanges with the commissioners where, you know, they basically said that, you know, what we did was similar to, you know, a nuclear warhead being dropped. I mean, I'm not making it up. And so that, the significance of that statement from a regulator who had the power to really hammer us hard, you know, stunned my general counsel.

Even those respondents not involved in previous FTC actions cited incidents such as those involving Choicepoint, Microsoft, Tower Records, Geocities, and other "FTC governance-type issues," as instigators for their firms' decision to hire a privacy officer, or create or expand a privacy leadership function. One described the threat of FTC oversight as a motivating "Three-Mile Island" scenario. Several described, moreover, the way in which the prospect of an enforcement action enhanced their credibility within their firm. "You know," said one,

> you had to start with the fear aspect or with the risk aspect. You can't really go in and build I think solely from an appeal to the . . . greater good, because it's not as tangible. It's longer term, right, and it's hard to do things in corporate America that are purely longer term. So I think you start with, boy, if we don't protect this, we're going to lose trust, we're going to-- and we could get prosecuted, you know?

"I walked in [to the firm]," described another, saying, "Look at what happened to them. This could be you. Be lucky because it's not just because they're bad guys. . . . And it was the FTC oversight [of other firms] and the length of scrutiny and the cost of audit that they had to submit to that I think was the dollar lever that started to open that box for me."

The very unpredictability of future enforcement can lead, a different respondent described, to "good dialogue" with regulators. "I think," she said, that "companies are often reticent to expose what they're doing for risk that they will be, you know, investigated or somehow found lacking. I would rather have the conversation now than have it during an enforcement action." Indeed, another suggested: "take a look at the FTC enforcement actions" under a

> loose framework of section 5. . . . [T]hat extra layer of – I don't think any privacy officer wants to skirt with – unless there is a compelling need. You have to

> analyze that in terms of the strict compliance line versus what can we do above and beyond that that's appropriate.

Similarly, another respondent remarked on the way that respondent's interactions had revealed differences between the FTC and European privacy regulators, reflecting the effects on U.S. business of the threat of, yet uncertainty about, FTC enforcement:

> You know, it's kind of funny in Europe where they get all kooky about the Americans who want to dot every I and cross every T. And it's like, well I'm sorry, my enforcement agency which is the Federal Trade Commission, they enforce the, you know, the black letters, [but also] the spaces, the semicolons, the periods; all those things are things they enforce.

b. Data Breach Notification Statutes

In addition to the changing role of the FTC, every single respondent mentioned a second regulatory development, the enactment of state data breach notification statutes,[60] as an important driver of privacy in corporations. . These laws, the first of which took effect in California in 2003, require that companies disclose the existence of a data breach to affected customers, usually in writing.[61]

Such laws, respondents explained, have served as a critical attention mechanism, transforming the effects of media coverage, and heightening consumer consciousness. "[A]ll the news around security breaches" is "[a] large focus," reported one respondent. In the words of another, "the breach news in the states last year was so--the drumbeat was so loud--that it didn't take much to get the attention of our senior executive on data security, kind of as part of the privacy program."

This mechanism has called attention specifically to the effect of the treatment of personal information on consumers:

> "it sure has heightened more people's understanding of the stakes inherent in managing data in a very real way" by "shift[Ing] the thinking of thinking about risks inside the company from thinking about the risk of losing data of IP or financial information, never thinking about the rest of the poor individual--I just lost a credit card file, okay, I lost a credit card file, who gives a hoot, but you know, it's capped, so no big deal, now, holy moly, I lost somebody's social security number and now there's liability associated with it for the company and they have to worry about it."

---

[60] As of December 9, 2009, forty-five states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information, *see* National Conference of State Legislatures Website, at http://www.ncsl.org/default.aspx?tabid=13489.

[61] *See e.g.*, Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82. State laws differ to some degree on issues such as permissible delay, penalties, the existence of private rights of action, and the existence of exemptions for breaches determined "immaterial."

The public attention triggered by notification requirements has been critical, several respondents reported, in strengthening the privacy function more generally. Notification legislation, reported one, "enriched my role; it's putting more of an emphasis on leadership internally in a very operational sense as opposed to just policy setting and management of that sort." Indeed, explained another,

> the external environment has helped that tremendously. And that's everything, you know, from what the CEO reads in the newspaper to the number of breach letters that our own employees and executives get from other companies saying, "Oh, my gosh, I don't want this happen to us. I don't want to see one of these with [our company's] logo on it," you know. So I think there has been a lot of pressure in the U.S. media, particularly on the data breach issue, but then that gave me the opportunity, internally, to say, "Well, it's not just data breaches, it's not just laptops, it's a responsible overall program about how we take in, and use, and process and secure data. . . . it's a tiny little, you know, the tip of the iceberg, really of, you know, what privacy challenges are, and the privacy program should be."

At the same time, however, a respondent who heads privacy at a global company discussed her perception that many European companies, despite their more rigorous FIPPS compliance requirements, are far less sensitive to the problems of compromised data when they outsource business functions. They "don't think about it very much," she said, because "[t]hey don't have security breach notification," which "changes behavior."

2. Legal Changes and the Court of Public Opinion

The high-profile activities of FTC and the disclosures mandates by breach notification law, our respondents explained, were particularly important because they dovetailed with already-occurring social and technological changes fueling privacy consciousness. This rise in consciousness both germinated, and was in turn facilitated, by the growth in media interest in privacy, and the development of what one called a "privacy community"—including advocates and journalists—that pressed privacy as an issue. Respondents thus described the way in which the "court of public opinion," as well as regulatory attention, is shaped by "a nice, close loop that is the media advocate," and stressed the importance of "what the CEO reads in the newspaper" to the "external environment."

"[R]ight now," explained one,

> you see the "P-word all over the place. You know, it used to be like once a week I'd cut out an article and say, "Look, they're talking about privacy in the paper on page twenty-two of the Wall Street Journal." And now it's pretty much every day. So I think we've won the battle of actually being noticed."

Indeed, said another, "I think seeing other big brand names take a hit on the issue certainly raised awareness." These developments, in turn reflect a what a third termed a "growing sensitivity by particularly senior executives to [privacy] things that are going on in the marketplace."

Thus,

> companies have seen that there is a lot of news about it and it can be a help to them in terms of figuring out PRM activity, avoid the bad and promote the good. Try to avoid the breaches and the problems and the brand tarnishment issues and promote the ability to use and flow data in a proper way and make it a competitive advantage for him.

3. The Role of Professionalization in Filling in Ambiguous Definitions of Privacy

The consequent empowerment of those responsible for privacy within firms was, in turn, amplified the role of the increasingly professionalized privacy-officer field in shaping the dynamic, consumer-protective approach to privacy. One CPO summed it up by stating,

> Part of the privacy office challenge is what I call demystifying privacy . . . typically your boss and your bosses boss don't have a good, you know, pre-established idea of exactly what the program will look like except that they want a good one. That's what my bosses said, we want to have a wonderful privacy program and you tell us what that means. I think that's not an unusual experience.

In defining what "a wonderful privacy program means" in the face of a quickly-moving regulatory target, an active advocacy community with effective public-relations skills, and shifting norms arising from changes in technology and its use by consumers, the interviewed privacy leaders revealed a deep reliance on peers.

Specifically, interview responses highlighted the role that professional associations and communities of practice play in "filling in the details" of a fluid consumer-expectations privacy mandate. The importance of the IAPP, the large privacy trade association described earlier in Section I, was made explicit. The association's publication and dissemination of information as to best-practices approaches, and its capacity to provide a space for "networking," and "getting to see the other privacy offers" one respondent said, is about getting "drenched in the culture." Respondents reported that a non-trivial component of their job duties involved collaboration with other members of the privacy sector, and information-sharing about accepted best practices, guidelines and policies among the CPOs we interviewed was rampant.

Information garnered from peers provides privacy officers both with leverage as they advocate for certain privacy practices within their own firms, and with an important cost-savings technique for allowing CPOs to draw on the information and insights generated by better financed peers. Information-sharing, one CPO stated, "is really helpful for very resource-strapped groups . . . . [I]f there's a change in privacy, it's so ill-understood outside of our little enclave that for me to say, 'I need five hundred thousand dollars to do a research project based on opt in'—it ain't happening." To fill the knowledge gap within the constraints of the corporate budget, CPOs report learning from those they perceive as leaders—"So, with other corporate leaders, you know, the Microsofts and the Axioms and the P&Gs and others who really have phenomenal programs, there's a lot of, I think, of sharing that goes on."

At times, the peers themselves were literally brought into an intra-firm conversation. Strikingly, one CPO reported,

> I've been on the phone with [other firms'] executive committees, telling them about [our company's] experience because it helps the other company, you know, privacy office to have me tell their people because they've told them and they don't believe them. So when they hear it directly from me, that has some advantage and I've done that with a number of different companies. And we just see that we have to go down this path together. It's very important.

Thus while doing privacy "well" was viewed by respondents as a strategic advantage in the marketplace, those respondents generally expressed the view that a peer's mistake risked tarnishing the entire sector or worse, by drawing regulatory or public attention. For this reason, CPOs reported that helping competitors to make better privacy decisions was in her interest. In the words of one:

> if I help my competitor at XYZ company do better I don't think that's about competitive advantage. That's about doing the right thing because if they screw up, you know what, it screws up all of us.

Similarly, another respondent attributed a willingness to share information about privacy policies and practices quite freely to that respondent's belief that privacy offered more value to an industry space than to an individual firm. This perceived lack of competitive value created tremendous latitude for information sharing:

> I think most companies have the belief that the best practice, the good privacy statement or the training materials, you know, a process for handling a security breach isn't going to give you a competitive advantage and—but, you know, so you share these things pretty freely. We are pretty much an open book. If I had created it, then I'm very happy to share it pretty much with anybody, regardless of what it is, for the most part.

III. CONTEXTUALIZING THE INTERVIEWS—AN ACCOUNT OF PRIVACY ON THE GROUND

The accounts of interviewed privacy leaders strengthen the quantitative external evidence of a radical increase in corporate privacy management between Smith's study and ours. By their descriptions, privacy took on new meaning during this era; in response firms evolved new management practices. These practices, moreover, address many of the failings Smith identified, namely systemic inattention to privacy, reactive policy development, and gaps between policy and practice. Yet they emerge without the passage of comprehensive federal privacy laws or the creation of a U.S. data protection authority. And most notably, the new definition that they claim organizes privacy thinking is characterized by less, rather than more, legal specificity, directly counter to the reduction in ambiguity that Smith championed.

If the developments were not spurred by the introduction of an omnibus privacy law and data protection agency—for in fact the U.S. held fast to its piecemeal approach to federal privacy legislation during this period of change—what was the context in which they occurred?

The interviews suggest that changes in the logic and practice of corporate privacy management tracked other atmospheric, institutional and substantive developments—developments that play a minimal role in dominant critiques of the U.S. privacy framework. Specifically, they suggest that a constellation of regulatory phenomena—the emergence of new activist federal regulators, new information-forcing state laws, and the increased visibility and influence of privacy advocates in the regulatory landscape—fostered legal and market connections between privacy, trust and corporate brand, which combined with the professionalization of privacy officers to heighten attention to privacy management within corporate America.

In light of these suggestions, this Section explores those phenomena, and details the history of their development. This account reveals a history of purposeful interactions among regulators and other actors across the U.S. privacy field to shape the logic of privacy protection in ways reflected by the interview responses. While a language of "trust," and the connection between privacy and consumer protection, first arose on the global stage during the early days of the commercial internet, the emergence of the Federal Trade Commission as a site of privacy norm interpretation pursuant to its broad Section 5 authority built upon the broader conversation of privacy as a market enabler. The FTC's activities were neither driven nor limited by standard data protection rules, but took advantage of breadth and ambiguity in its statutory mandate, and the agency ultimately provided a forum for the expansion of privacy discourse. This forum, strengthened by privacy disclosures mandated by state security breach notification laws, enhanced the visibility of privacy debates, empowered a movement of privacy advocates, and strengthened the position of privacy professionals within corporate organizations. Leveraged by the agency's entrepreneurial use of its enforcement powers, and by increased market pressures for privacy performance these activities, these developments moved the privacy discourse from a focus on individual procedural mechanisms to an approach emphasizing the protection of substantive privacy norms, and shaped corporate privacy practice by creating a "realistic threat of retribution for inattention"[62]

A. The Roots of a Consumer-Focused Language Of Privacy

The privacy leaders we interviewed unanimously articulated a non-FIPPS-based definition of privacy as driving activity within their firms. Privacy was portrayed as an expansive concept: privacy "equates to trust," "is a strategic initiative," and "a core value associated with trust, primarily, and integrity and respect for people." Moreover the concept sounded in terms of broad principles: "apply[ing] information usage to new contexts" in a "very contextual" manner. And the implementation of these principles required ongoing expertise: "[T]he company . . . understands that trust plays a key part . . . but isn't able to kind of codify what . . . trust looks like," so "the idea that there's going to be a one-size-fits-all privacy practice is, I don't think, possible." Thus "you don't really have a practice that is uniformly developed on the back end because it's also a

[62] SMITH, *supra* note __ at 214.

judgment call." Finally, it was tied to consumer reputation: "the biggest value to privacy is it's a part of brand."

This way of framing privacy reflects a discourse that first arose in the mid-1990s, a transformative period for information and communication technology use and policy in the U.S. and globally. The birth of the internet as a commercial medium and the need to respond to privacy challenges created by its global and data-driven nature altered the political discourse about privacy protection. Specifically, in both the U.S. and in the European Union, arguments about the importance of privacy protection no longer sounded exclusively in the language of individual rights protection. Instead, they also reflected a desire to facilitate electronic commerce and the free flow of information by building consumer trust. While tension between the EU and the U.S. about how to instrument the protection of privacy was high, they increasingly advanced a similarly instrumental rhetoric about privacy's value, stating that electronic commerce "will thrive only if the privacy rights of individuals are balanced with the benefits associated with the free flow of information."[63]

By 1996, the rhetoric of consumer trust as a reason for business to attend to consumer privacy had become "something of a mantra" internationally.[64] That year, the Organisation for Economic Co-operation and Development (OECD)[65] issued the first in a series of reports indicating that "privacy interests" needed bolstering, not only for human rights reasons, "but also [to ensure] that the right balance is found to provide confidence in the usage of the system so that it will be a commercial success."[66] In preparation for the EU ministerial conference on Global Information Networks in Bonn in July 1997,

---

[63] White House, *Framework for Global Electronic Commerce* 12-14 (July 1, 1997),

[64] Bennett & Raab, *supra* note 1 at 49.

[65] A consortium of 30 countries, including the United States and many European countries, united in their commitment to democracy and a market economy. Organisation for Economic Co-operation and Development (OECD), *Members and Partners*, http://www.oecd.org/pages/0,3417,en_36734052_36761800_1_1_1_1_1,00.html (last visited Aug. 1, 2008) (describing what OECD does and who its members are).

[66] OECD, *Report of the Ad Hoc Meeting of Experts on Information Infrastructures: Issues Related to Security of Information Systems and Protection of Personal Data and Privacy* 8 (1996), http://www.oecd.org/dataoecd/32/50/2094252.pdf. Later reports continue this theme, *see OECD Ministerial Conference "A Borderless World: Realising the Potential of Global Electronic Commerce," Conference Conclusions* 5 (Oct. 1998), http://www.olis.oecd.org/olis/1998doc.nsf/LinkTo/NT00000FEE/$FILE/12E81007.PDF. (stressing that "users must gain confidence in the digital marketplace" and "that the potential benefits [of global electronic commerce] will not be realized if consumer confidence. . . is eroded by the presence of fraudulent, misleading and unfair commercial conduct."); *Declaration on Consumer Protection* and *Conference Conclusions* OECD, *Ministerial Declaration on Consumer Protection in the Context of Electronic Commerce* 3 (Oct. 1998), http://www.olis.oecd.org/olis/1998doc.nsf/LinkTo/NT00000E12/$FILE/12E81004.PDF (mentioning "trust" and "confidence" a total of twenty times in 19 pages but mentioning privacy rights once to declare that member nations will "ensure the respect of important rights" without stating a consensus position on what those rights are, or how they function in the marketplace).

German Economics Minister Günter Rexrodt and EU Commissioner Martin Bangemann wrote, "building confidence by achieving efficient [privacy] protection is essential to allow the positive development of these networks."[67] The organization's report on *Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet*,[68] also issued that year, concludes that "consumer confidence is a key element in the development of electronic commerce," and that enforcement of privacy policies serves to bolster that confidence.[69] On the domestic front the Clinton Administration released its white paper, *Framework for Global Electronic Commerce*, which stated that e-commerce "will thrive only if the privacy rights of individuals are balanced with the benefits associated with the free flow of information."[70]

Thus scholars in this period identified "an emerging international consensus" in the public and private sector "on the importance of trust and confidence in modern information and communication technologies and their application to online transactions."[71] The dominant reason advanced to protect privacy in high-level government statements on the global stage, was the promotion of electronic commerce rather than individual privacy rights.

B. The U.S.-E.U. divergence: The Timing of Institutionalization

While this instrumental expression of privacy's value in a networked world spanned the Atlantic, it encountered divergent regulatory climates in the U.S. and Europe. European countries were committed under the EU Data Protection Directive[72] to a rights-based implementing framework with local Data Protection Authorities (DPAs) to monitor its application.[73] The DPAs, some of whose existence dated from 1970's, were also organized around a rights-based framework.[74] Thus, in Europe the shift in privacy rhetoric occurred against a well-developed framework and growing set of institutional players committed to conceptualizing information privacy through a lens of "data protection."[75]

---

[67] Bennett & Raab, *supra* note 1 at 49.

[68] OECD, *Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet* 4 (May 22, 1998), http://www.oecd.org/dataoecd/33/43/2096272.pdf.

[69] *Id.*

[70] White House, *Framework*, *supra* note __ at 12-14 (describing privacy protection as essential, but that privacy should not inhibit the free flow of information; self regulation is the way). .

[71] Bennett & Raab, *supra* note 1 at 50.

[72] Available at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

[73] Directive, Article 28.1

[74] *See* ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 74-98 (2008) (arguing that the adoption of the EU Directive itself is rooted in the "historical sequencing of national data privacy regulation and the role that the resulting independent regulatory authorities played in regional politics").

[75] For a discussion of EU member states' laws and the process leading up to the directive, see, Fred H.Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33

By contrast, the information privacy landscape in the United States was more of a *tabula rasa*. Its patchwork system reflected no deep commitment to a specific implementation framework, and no institutional authority vested in defending a specific approach. Against this backdrop, the expression of privacy's value in terms of promoting consumer trust proved influential in the U.S. in a way that rights-based arguments had not. Historically, successful legislative efforts, with a few notable exceptions, were mounted in response to specific and egregious harms or to protect highly sensitive information. Advancing privacy as a matter of individual rights, generically, across the corporate sector, had little legislative or regulatory traction. By contrast, legislators and regulators were relatively quick to join a conversation about addressing privacy risks to advance electronic commerce.

Consumer confidence and trust became a central theme of arguments both for and against new privacy regulations in the U.S. On the one hand, consumer advocates employed such arguments in promoting a regime of new privacy laws. Advocates claimed that in the absence of robust privacy protection individuals would be "more fearful to disclose information"[76] and would retreat from shopping or banking online.[77] Consumer groups warned that "the full economic and social potential of global electronic commerce will only be realized through its widespread use by consumers," and "such use will only occur if consumers become confident and comfortable with the online world."[78] Business groups, on the other hand, employed this new rhetoric to support a self-regulatory agenda, stating that "building consumer confidence is a key issue for the development of electronic commerce"[79] and claiming "There is a business advantage to be gained by companies that safeguard consumer interests."[80] When the Federal Trade Commission sought public comments in preparation for a consumer protection workshop in 1999, sixty-nine companies, nonprofits and individuals responded—some in

---

INDIANA L. REV. 33 (1999).

[76] John Schwartz, *Health Insurance Reform Bill May Undermine Privacy of Patients' Records*, WASH. POST, Aug. 4, 1996, at A23 (quoting Denise Nagel of the National Coalition for Patient Rights, who was responding to the recently-passed Kennedy-Kassebaum health insurance reform bill, which mandated the creation of a national computer network among health care providers, who were required to participate).

[77] Robert O'Harrow Jr., *White House Effort Addresses Privacy; Gore to Announce Initiative Today*, WASH. POST, May 14, 1998, at E1.

[78] Letter from Frank C. Torres, III, Legislative Counsel to Consumers Union, to the Federal Trade Commission (Mar. 26, 1999), http://www.ftc.gov/bcp/icpw/comments/conunion.htm (these folks favor further rules and standards with regard to privacy, and they, too, use consumer trust to bolster their arguments).

[79] Global Business Dialogue on Electronic Commerce, *The Paris Recommendations* 6 (Sept. 13, 1999), http://www.gbd-e.org/pubs/Paris_Recommendations_1999.pdf (further evidence that the business community embraced at least the rhetoric of consumer trust).

[80] Alliance for Global Business, *Global Action Plan for Electronic Commerce* 22 (Oct. 1999), http://www.iccwbo.org/policy/ebitt/display7/folder85/index.html

favor of self-regulation, and others arguing for new rules, but nearly unanimous in stressing the importance consumer trust.[81]

The link between privacy, trust and commerce, moreover, was underscored by repeated consumer pushback after corporate privacy blunders. "Consumer concern about privacy [had] the attention of Corporate America."[82] Companies announced information-sharing deals only to cancel them once masses of consumers made their objections known.[83] In July 1997, AOL scrapped a plan to sell subscribers' phone numbers to marketers.[84] Other high-profile reversals followed: in 1998, American Express pulled out of a partnership with KnowledgeBase Marketing that would have made the personal data of 175 million Americans available to any retailer that accepted the charge card.[85] In 1999, Intel reversed a plan to activate an identifying signature in its Pentium III chip faced with advocacy filings with the Federal Trade Commission, pressure from industry partners, and a boycott.[86] And in 2000, a plan by DoubleClick, the dominant network advertising service, to combine clickstream information with personally identifiable information in a massive customer database it had acquired for the purpose of delivering highly customized and targeted advertising was shelved. DoubleClick withdrew its plan due to public pressure.

While disputes over the optimal way to build trust waged on—consumer advocates favoring a regime of new privacy laws, the Administration and industry groups favoring industry self regulation—all players increasingly framed their arguments in favor of privacy protection in instrumental terms—the crucial role privacy played in enabling electronic commerce and e-government. This fit well with the Administration's predilection for market driven solutions, the regulatory powers of the Federal Trade Commission which was staking out its agenda in the privacy space, and the agenda of pragmatic advocates keen to promote reforms by utilizing available regulatory fora.

C. Regulatory Developments and the Consumer-Oriented Privacy Frame

1. The Federal Trade Commission and the Consumer-Protection Discourse

---

[81] List of Commenters in Preparation for a Federal Trade Commission Workshop on U.S. Perspectives on Consumer Protection in the Global Electronic Marketplace (1999), http://www.ftc.gov/bcp/icpw/comments/ (listing all commenters and links to their comments; nearly every comment makes at least a passing mention of consumer trust before launching into their vision of privacy protection).

[82] Bruce Horovitz, *AmEx Kills Database Deal after Privacy Outrage*, USA TODAY, July 15, 1998, at 1B (describing the scrapped AmEx deal, and at the end of the article listing other companies "that recently changed course after consumers balked").

[83] *See, e.g., id.*

[84] *Id.*

[85] *Id.*

[86] Jeri Clausing, *The Privacy Group that Took on Intel*, N.Y. TIMES, Feb. 1, 1999, at C4 (describing a successful grassroots campaign to force Intel to reverse its plans to activate an identifying signature in the Pentium III chip).

It is in this context that the Federal Trade Commission emerged,[87] in the words of one of our respondents, as an "activist privacy regulator," engaging the broader privacy community in a conversation about privacy's meaning through its consumer-protection lens.[88] "We recognized," explained former FTC Chairman Robert Pitofsky, speaking about his time at the agency, "that the Internet was a vast new marketplace that could provide great benefits to consumers and to the competitive system. The idea was to protect consumers without undermining the growth of electronic commerce. A special dimension of commission activities related to concerns about on-line privacy."[89]

a. Jurisdictional Entrepreneuship

This development was not predetermined by the terms of the Commission's statutory mandate to police "unfair or deceptive acts or practices."[90] As Jodie Bernstein, Director of the FTC's Bureau of Consumer Protection from 1995-2001, remarked, "It didn't quite fit into 'deception or unfairness' for us to say, 'Everybody out there ought to be required to protect people's privacy.'" [91] Thus, she explained, "I didn't go through any big deal process in terms of saying, 'Yes we're policing the Internet.'"[92] But the

---

[87] The FTC had developed expertise on privacy as the agency responsible for rulemaking and enforcement under several sectoral statutes including, Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (addressing the accuracy, dissemination, and integrity of consumer reports); Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6101 et seq. (including the Telemarketing Sales Rule, 16 C.F.R. Part 310) (prohibiting telemarketers from calling at odd hours, engaging in harassing patterns of calls, and failing to disclose the identity of the seller and purpose of the call); Children's Online Privacy Protection Act, 15 U.S.C. § 6501 et seq. (prohibiting the collection of personally identifiable information from young children without their parents' consent); Identify Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 (directing the FTC to collect identity theft complaints, refer them to the appropriate credit bureaus and law enforcement agencies, and provide victim assistance). For an overview of the FTC's power's under specific grants of authority, including several enacted during the late 1990s, *see* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW, 777-82 (2009) and RICHARD C. TURKINGTON AND ANITA ALLEN-CASTELLITTO, PRIVACY LAW: CASES AND MATERIALS, 428, 476-488, 492, 496-500 (2002).

[88] *See, e.g.*, Christine A. Varney, Commissioner, FTC, Prepared Remarks on *Privacy in the Electronic Age* at the Privacy & American Business National Conference (Nov. 1, 1995)http://www.ftc.gov/speeches/varney/varnprvy.sthm (making the point that the FTC is grappling with questions about how best to approach privacy in the information economy).

[89] Oral History of Robert Pitofsky Sixth Interview March 30, 2004 p. 155.

[90] 15 U.S.C. § 45.

[91] Oral History of Joan (Jodie) Z. Bernstein – Seventh Interview, May 1, 2000 p. 240. For an overview of the FTC's activities through 1996 see, Consumer Privacy on the Global Information Infrastructure, Staff Report, Federal Trade Commission (1996), for an overview of completed and planned work as of 1999 see Self-Regulation and Privacy Online, Prepared Statement of the Federal Trade Commission, presented by Chairman Robert Pitofsky before the Subcommittee on Communications of the Committee on Commerce, Science, and Transportation, United States Senate July 27, 1999.

[92] *Id.*

substantive imprecision and procedural breadth inherent in the FTC Act left the agency the space to play an increasingly important role in framing the debate. "There were internal discussions about how to handle it," Bernstein continued, "and from that came our concept of convening forums on privacy issues on the Internet very early and to articulate our program. Then we did the first survey of what was happening to the personal privacy on the web sites, encouraging self- regulation, [and learned that] the privacy issues are real hot right now."[93]

Thus, beginning in 1995 with a public workshop to identify the consumer protection and competition implications of the globalization and technological innovation at the core of the internet revolution, and continuing with similar programs over the following several years, the FTC began to chart its own privacy agenda.[94]

These initiatives were strengthened as the EU Data Protection Directive's effective date of 1998 loomed, and the issue of the "adequacy" of U.S. law became a pressing trade matter. In light of the Directive's prohibition on the transfer of data to companies in jurisdictions which failed the test of "adequacy"—which included as the United States—U.S.-based multi-nationals, and other firms with a global presence, or substantial foreign markets feared the economic consequences. These fears led to the initiation of negotiations to develop a "safe harbor" framework, by which individual U.S. firms could sign-on and thereby demonstrate privacy practices sufficient for trade with European partners.[95] These negotiations culminated with the EC approval of the "Safe Harbor Privacy Principles" (Safe Harbor) in July 2000.[96]

Throughout the extended and contentious process of negotiating the Safe Harbor agreement heavy pressure was on U.S. industry to evidence meaningful capacity to self-regulate and for the U.S. to provide evidence of meaningful oversight, enforcement and mechanisms for redress. Struggling with the need for credible oversight and enforcement structures for privacy, but unwilling to craft either omnibus regulations or to push for the creation of a data protection authority, and faced with limited industry support and participation in self-regulatory activities with credible enforcement, the Administration and industry turned to the Federal Trade Commission to fill this gap. A critical component of the Safe Harbor Agreement, then, was the commitment by the

---

[93] *Id.*.

[94] For an overview of the FTC's activities through 1996, see Federal Trade Commission, Staff Report, *Consumer Privacy on the Global Information Infrastructure* (1996); for an overview of completed and planned work as of 1999, see *Prepared Statement of the Federal Trade Commission: Self-Regulation and Privacy Online*, presented by Chairman Robert Pitofsky before the Subcommittee on Communications of the Committee on Commerce, Science, and Transportation, United States Senate (July 27, 1999).

[95] For an in depth discussion of the connection between the EU Directive and privacy developments in the U.S. and other countries see Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMP. L. & SECURITY REP. (2008).

[96] http://ec.europa.eu/dgs/internal_market/mission_en.htm (Last visited May 7, 2009)

Federal Trade Commission to enforce privacy statements and to prioritize complaints by EU citizens.[97]

With the Safe Harbor's signal, the FTC was now relatively insulated against suggestions that its nascent privacy activities were beyond its inherent authority. The Federal Trade Commission became a laboratory of privacy norm elaboration, seeking through its own and outside expertise, measurement, investigation, and sustained stakeholder engagement to define privacy's place in the new online market place, and its role as the leading consumer protection agency in shaping and enforcing practices to respect it.

The FTC was neither bound to, nor enabled by, traditional conceptions of data protection—for better and worse. However, it had substantial discretion to define what practices were unfair and deceptive.[98] As the Supreme Court observed as early as 1931, unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by . . . 'the gradual process of . . . inclusion and exclusion.'"[99] For "[n]either the language nor the history of the Act suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories."[100]

The agency, further, possesses wide latitude as to the institutional methods available for developing its perceptions of legal requirements. In the privacy arena, the FTC used convening and fact finding powers to facilitate a dialogue about corporate data practices, consumer understanding and expectations, and consumer harms. It convened Federal Advisory Committees[101] and workshops,[102] requested[103] and issued[104] reports,

---

[97] Article 1 ¶ 5 of the EC's Commission Deicison explicitly provides that " the organisations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce, or that of another statutory body that will effectively ensure compliance with the Principles." (EC Commission, July 27, 2000). *See also* Priscilla M. Regan, *Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows*, 59 J. SOC. ISS., 263-282 (2003) (discussing national and international politics related to the adoption of the Safe Harbors).

[98] See Federal Trade Commission Act, 15 U.S.C. § 41 et seq. (prohibiting deceptive or unfair acts or practices), and Federal Trade Commission, *Statement on Unfairness* "The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time"); Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305 (2001) (discussing congressional delegation and court deference that results in FTC's ability to define deceptive practices); Jeff Sovern, *Private Actions Under the Deceptive Trade Practices Acts: Reconsidering the FTC Act as Rule Model*, 52 OHIO ST. L.J. 437, 440-45 (1991) (discussing FTC's broad interpretative authority).

[99] *FTC v. Raladam Co.*, 283 U.S. 643, 648 (1931).

[100] *FTC v. R.F. Keppel & Bro.*, 291 U.S. 304, 310 (1934).

[101] *See, e.g.*, Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security, May 15, 2000.

worked with industry to develop self-regulatory codes of conduct,[105] and employed its enforcement powers to ratchet up demands on industry to be transparent about privacy practices, respect consumer understandings, and safeguard personal information.[106]

In contrast to the static requirements and prohibitions of U.S. sectoral statutes, FTC actions presented industry with an evolving set of privacy "norms," as the agency, in conjunction with the cadre of experts empowered by its activities, developed understandings of the meaning of privacy as a trade practice. The agency's broad statutory authority and its expansive institutional powers contributed to a growing imprecision about what it meant to satisfy the rhetorical measures of "privacy protection" and "consumer trust" in the online environment.[107] This, in turn, accorded the agency substantial capacity to shape the terms of the debate in a dynamic fashion.

b. Developing a Consumer Expectations Metric

i. Non-Enforcement Regulatory Tools

---

[102] The agency held fourteen public workshops on matters related to privacy between 1995 and 2004. Twelve related to unfairness and deception, one concerned financial privacy, and one credit reporting. *See* ftc.gov, Unfairness and Deception: Workshops, *available at* http://www.ftc.gov/privacy/privacyinitiatives/promises_wkshp.html; Financial Privacy: Financial Privacy Rule: Workshops, *available at* http://www.ftc.gov/privacy/privacyinitiatives/financial_rule_wkshp.html (last visited Feb. 27, 2010); ftc.gov, Credit Reporting: Workshops, *available at* http://www.ftc.gov/privacy/privacyinitiatives/credit_wkshp.html

[103] *See, e.g.*, Report to the Federal Trade Commission by the Ad-Hoc Working Group on Unsolicited Commercial Email (1998).

[104] Since 1996 the agency has issued seventeen reports relating to privacy. The agency has issued seven staff reports and ten reports to Congress. *See* ftc.gov, Unfairness and Deception: Reports and Testimony, *available at* http://www.ftc.gov/privacy/privacyinitiatives/promises_reptest.html; ftc.gov, Financial Privacy: Pretexting Reports and Testimony, *available at* http://www.ftc.gov/privacy/privacyinitiatives/pretexting_reptest.html; ftc.gov, Children's Privacy: Reports and Testimony, *available at* http://www.ftc.gov/privacy/privacyinitiatives/childrens_reptest.html.

[105] *See* FTC, *Individual Reference Services: A Report to Congress*, (1997); *Network Advertising Initiative: Self-Regulatory Principles For Online Preference Marketing By Network Advertisers* (2000).

[106] *See generally* Chris Jay Hoofnagle, *Privacy Practices Below the Lowest Common Denominator: The Federal Trade Commission's Initial Application of Unfair and Deceptive Trade Practices Authority to Protect Consumer Privacy (1997-2000)*, (January 1, 2001) (discussing the initial 5 cases brought by the FTC under their deceptive practices act jurisdiction).

[107] *See* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2053-54 (2001) ("The Agency has provided very little information, however, which would indicate the standards of fairness the Agency intends to apply," and therefore businesses have "little guidance as to how much is required of them in terms of providing notice, data security, data access, and determining what constitutes consent.").

Central to the FTC's emerging role as privacy regulator was its employment of regulatory tools outside the enforcement context, notably publicity, research, best-practice guidance, the encouragement of certification regimes, the enlistment of expert input, and other deliberative and participatory processes promoting dialogue with advocates and industry.[108] These tools furthered three types of regulatory goals.

First, they greatly increased the transparency of corporate privacy practices. Prior to these activities the invisibility of corporate practices, as noted by Smith's 1994 study, made them largely immune to regulatory and public pressure. FTC initiatives brought corporate practices into the light, and fueled a sustained debate about appropriate corporate norms of behavior on an issue that was previously addressed episodically, at best, by legislators in response to high profile privacy failures.

The agency conducted "sweeps" of both child-directed and general audience web sites to assess information practices. It encouraged stakeholders to engage in their own research to document privacy practices on the internet which led to additional surveys of business practices online and consumer expectations. This focus on fact finding about corporate practices provided pressure for continuous improvement on industry, as initial sweeps provided a baseline for measuring improvement, or at times the lack thereof. The emphasis on best-practice improvement in turn provided an important tool for trade associations and self-regulatory organizations to use in corralling the business community to join forces to stave off the threat of regulatory action. Through a variety of measures, the Commission thus focused on developing a detailed public record of factual data about privacy-impacting technologies and related business practices, and how these practices in turn related to consumers' expectations and privacy concerns.

Second, the Commission employed its bully pulpit power to motivate two important developments. Its calls for credible self-regulatory efforts that provided meaningful redress for consumers and oversight and enforcement of policies were largely responsible[109] for the creation of two self-regulatory privacy seal programs[110] as well as a technical standards designed to reduce the transaction costs associated with privacy decision making by standardizing and automating the process.[111] Furthermore, Commission persuasion was critical in encouraging companies operating online to post

---

[108] *See generally* Kenneth A. Bamberger, *Normative Canons in the Review of Administrative Policymaking*, 118 YALE L. J. 64, 99-100 (2008) (discussing the capacity of agencies to provide a site for norm elaboration through deliberative and participatory processes outside the APA rulemaking or adjudication processes).

[109] Ongoing negotiations with the European Union over the "adequacy" of U.S. companies' privacy practices and U.S. law led to the creation of the Safe Harbor Guidelines. Companies that subscribed to the Guidelines would be considered to have adequate privacy protection for the sake of EU law and therefore would be able to receive data on EU citizens. In this context too, proving that remedies were available and that industry would be regularly policed through some oversight body was an important component of the agreement. Thus, the Commission's work was not the sole contributor to the creation of the seal programs.

[110] Truste, BBBonline.

[111] P3P, Tim Berners Lee & Deirdre K. Mulligan FTC presentation; Lorrie Cranor; Lessig.

privacy policies. The Commission's workshops and presentations, combined with publicity about privacy invasions occurring online, fueled this pressure. As discussed below, the publication of policies making representations about companies' practices with respect to personal information became central to the Commission's initial exercise of its Section 5 enforcement jurisdiction, because the least controversial manner for the FTC to exercise authority in the privacy area was to address factually misleading claims.[112] In addition to fueling the FTC's assessments, the visibility into corporate practices these policies provided facilitated a measurement of corporate privacy practices by legislators, advocates, and the press.

Finally, the FTC's participatory fora provided a space for a sustained conversation about privacy outside the bright lights of the congressional hearing rooms that empowered privacy advocates. Never before had privacy claimed a domestic institutional home as well resourced as the FTC, and the advocacy community quickly took advantage of the FTC's heft, filing numerous complaints about business practices[113], participating in Federal Advisory Committees[114] and workshops, and engaging in agenda-setting through the production of independent research[115] as well as interactions with FTC staff and Commissioners. The agency's policy fora provided low-cost, and relatively high profile, opportunities for advocates to shape the discourse about corporate data practices. Indeed, several privacy organizations and advocates appeared on the scene in the mid- and late-1990's focusing much, if not all, of their energy on FTC engagement.[116] Workshops accorded an opportunity for advocacy organizations to convey their views to

---

[112] *See* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2046 (arguing based on public choice theory the FTC's promotion of privacy policies should be viewed as a means for "the Agency to sink its jurisdictional hooks more firmly into the Internet privacy debate, and therefore the Internet").

[113] *See, e.g.*, *Website*, ftc.gov (including press releases discussing five agency enforcement actions—against CVS Caremark, UMG Recordings, Microsoft, Eli Lilly, and Lisa Frank—initiated after privacy advocates or the media brought the matter to the FTC's attention) http://www.ftc.gov/opa/2009/02/cvs.shtm; BENNETT, THE PRIVACY ADVOCATES, *supra* note __, at 124-25, 152, 155, 160-61 (discussing four other actions triggered by complaints from advocacy groups.).

[114] *See, e.g.*, FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY-REPORT TO THE COMMISSION (May 15, 2000) (report of committee discussing mechanisms to afford consumers access to personal information collected and maintained by commercial Web sites, including representatives from Consumers Union, the Electronic Privacy Information Center, the Center for Democracy and Technology, the Electronic Frontier Foundation, as well as several privacy academics).

[115] *See, e.g.*, Center for Media Education, Report, WEB OF DECEPTION: Threats to Children from Online Marketing (1996); *Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial Email* (1998).

[116] For example, Junkbusters, a for-profit, privately held privacy advocacy firm founded in 1996, focused much of its activity on the FTC, *see* Amy Borrus, *The Privacy War of Richard Smith*, BUSINESSWEEK (Feb. 14, 2000) (containing FTC comments on the importance of Junkbuster founder Richard Smith's work).

a DC audience of reporters, hill staff, trade associations, lobbyists and industry executives. These contexts provided a formidable stage for advocates to serve as a mouthpiece for concerns about privacy risks faced by the diffuse and broad-based population of consumers nationwide.[117]

Advocates filed a steady stream of complaints with the FTC requesting investigations of corporate privacy practices testing and advancing the FTC's use of its deceptive and unfairness jurisdiction. [118] This level of activity contrasts starkly with advocates' pursuits in the far-more-costly realm of litigation; indeed, privacy organizations have rarely led court challenges to remedy privacy wrongs in the corporate sector.[119] Through a compelling FTC complaint an advocacy organization could leverage the resources, expertise, and investigative and enforcement capacity of a formidable agency. The publicity surrounding the filing of an FTC complaint could generate substantial scrutiny of corporate practices and might yield a related benefit by increasing the influence of the advocacy organization on the hill.[120] These complaints thus accelerated the dynamic the framing of privacy obligations, advancing from straightforward allegations of deceptive statements and unfair data practices[121] to novel complaints, such as those alleging that the assignment of unique identifiers to consumers' computers violated their expectations by putting them at unavoidable risk of

---

[117] *See generally* MANCUR OLSON THE LOGIC OF COLLECTIVE ACTION (1965) (articulating the public choice insight that concentrated groups enjoy a comparative advantage with respect to their ability to organize to advance group interests compared to groups facing diffuse, individually small benefits); George Stigler, *The Theory of Economic Regulation*, 2 Bell J. of Econ. & Mgmt. Sci. 3, 3 ((1971) (setting forth a model of interest groups and regulatory agencies by which "regulation is acquired by the industry and is designed and operated primarily for its benefit").

[118] The Center for Media Education (CME) filed the first internet related petition in May 1996, requesting that the FTC investigate Kidscom.com. While the FTC did not to file an enforcement action, its published letter evaluating Kidscom.com provided early notice of the agency's views on corporate data collection of children's information. *See* Letter from Jodie Bernstein, Director, FTC Bureau of Consumer Protection, to Kathryn C. Montgomery, President, Center for Media Education (Jul. 15, 1997) (concluding that collecting personally identifiable information from a child for a particular purpose when the information also will be used for another purpose that parents would find material, is a deceptive practice in the absence of a clear and prominent notice to a parent regarding the practice; and finding that parental consent must be obtained before a Web site that has collected identifiable information about children can release it to third parties) *available at* http://www.ftc.gov/os/1997/07/cenmed.htm *See also* BENNETT, THE PRIVACY ADVOCATES, *supra* note __, at 124-132 (discussing complaints in context of "naming and shaming" strategies); *id.* at 150-159 (discussing complaints against Intel, PSN, Doubleclick, and Microsoft Passport).

[119] *See id.* at 119-121.

[120]

[121] *See, e.g.*, *ACLU Complaint* (contending that Eli Lilly's disclosure of the email addresses of individuals receiving updates about Prozac constitute unfair trade practices in violation of section 5 of the FTC Act), *available at* http://www.aclu.org/technology-and-liberty/aclu-letter-ftc-re-eli-lilly.

privacy harms,[122] or targeting spyware and adware distributors, leading to enforcement actions discussed below.

In these fora, the FTC built support for its work and gained an ongoing awareness of the concerns of consumer advocates, and the ways in which consumer harms can arise from the breach of expectations wrought by the increased capacity and regularity of data collection—and a means publicizing them. Simultaneously advocates had a singular opportunity to shape an ongoing stakeholder dialogue in which the link between privacy, trust, and consumer expectation were nurtured—giving evolving content to imprecise rubric of privacy as consumer protection.

ii. Bringing Investigation and Enforcement Powers to Bear

These evolving consumer-oriented notions of privacy protection, in turn, were ultimately given force through the FTC's enforcement authority. As discussed above, the Commission's early cases focused on the accuracy of notices, targeting claims that were actively misleading. Then-Chairmen Pitofsky took a conservative view of the FTC's authority distinguishing the FTC's authority under section 5 from federal privacy statutes that "apply whether or not a privacy policy is posted" stating that "[o]nce posted, the privacy policy falls under the jurisdiction of the FTC, which uses existing laws to hold companies to the promises they make to consumers. In short, if a private sector web site does not post a privacy policy, there is no ready legal recourse available to an individual whose privacy has been violated."[123] Early enforcement actions followed suit, focusing on adherence to public statements related to a limited set of FIPPS principles tied directly into the creation of a functioning market for privacy that would limit the need for additional regulatory intervention—notably requirements of notice and consent.

This approach accorded with industry's expectation of the agencies exercise of authority. However, many in the privacy community pointed out the perverse disincentive this created for corporations to post privacy policies as it directed the FTC's action to what many believed would be the relatively good actors. As Joel Reidenberg wrote, "In an ironic twist, this public enforcement also provides a disincentive for greater

---

[122] *See* See In the Matter of Intel Pentium III Processor Serial Number: Complaint and Request for Injunction, Request for Investigation, and for Other Relief filed by the Center for Democracy and Technology, Consumer Action, and Privacy Rights Clearinghouse, *available at* http://netdemocracyguide.net/privacy/issues/pentium3/990226intelcomplaint.shtml.

[123] Remarks of FTC Chairman Robert Pitofsky, Hearing On Recent Developments In Privacy Protections For Consumers, House Subcommittee On Telecommunications, Trade And Consumer Protection (Oct. 11, 2000). Thus while two early investigations, one involving children, *see* FTC Guidance Letter in kids.com, *available at* http://www.ftc.gov/os/1997/07/cenmed.htm, and the other an anti-competitive practice that used personal information harvested from a competitors site in contravention of terms of service, s*ee* FTC Complaint in reverseauction.com inc, *available at* http://www.ftc.gov/os/2000/01/reversecmp.htm, included unfairness claims based on the inability of consumers to avoid substantial injury, the majority of early claims focused on affirmative misstatements of companies' data collection, use and disclosure practices.

transparency. A company risks liability by making a disclosure, but does not risk accountability by remaining silent."[124] The inability to police practices in the absence of a posted policy, accordingly, was perceived by advocates as an unacceptable gap in privacy protection.

As political support for improved privacy practices grew, resistance from industry waned—perhaps due to the FTC's central role in reducing tensions with the EU over cross-border data flows— and the perceived inequity of "extra policing for the good guys", the FTC approach broadened. The agency increasingly directed its enforcement focus on practices deemed "unfair"[125] and transactions that were on the whole misleading despite legal disclosures. This change in regulatory approach unraveled settled understandings of the agency's requirements regarding corporate privacy practices. If earlier enforcement actions aimed at holding companies to their word provided some precision as to rules of conduct, the new legal standards employed by the agency to protect privacy in the face of new technologies, new corporate behaviors, and new threats, were far more ambiguous, evolving, and context-dependent. This development is seen strikingly in the agency's actions to address two phenomena: spyware, and data breaches.

Spyware—a type of software that is typically installed on a computer without the user's knowledge, and collects information about that user—presented an important conceptual challenge to the FTC's policing of privacy, and to industry intent on distinguishing the good actors from the bad through adherence to procedural regularity. Companies distributing spyware often relied on the same fine-print legal disclosures as other companies to inform consumers of their data practices. The difference was that their practices diverged even further from consumers' expectations of the bargain they were striking than those of other market participants, and therefore put consumers at risk. No longer did it make sense that providing a legal disclaimer and click-through "consent" screen should suffice to evade FTC scrutiny.

In a series of actions against companies that downloaded software without appropriate notice and consent procedures[126] the Commission began to breathe substance into the process of consent. The majority of these cases involved "bundled software,"[127] where formal disclosures in end user licensing agreements (ELUAS) were

---

[124] Joal R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 Hastings L. J. 886, 886 (2003).

[125] *See, e.g.*, FTC v. GM Funding, Inc., et al. (C.D. Cal. 2002).

[126] FTC v. Seismic Entm't, Inc., 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004) (holding FTC was likely to succeed on the merits because it is an unfair practice to exploit a known vulnerability in the Internet Explorer web browser to download spyware to users' computers without their knowledge and enjoining this method of software distribution); Analysis of Proposed Consent Order to Aid Public Comment, *In re* Advertising.com, USFTC File No. 042-3196 (Aug. 3, 2005) (holding failure to clearly and conspicuously disclose bundled software that traced browsing deceptive); *see also* Complaint, FTC v. Odysseus Mktg., Inc., No. 05-CV-330 (D.N.H. Sept. 21, 2005) (alleging that failure to clearly and conspicuously disclose bundled software with security and privacy risks is deceptive).

[127] In "bundled" software offerings, the user understands that they are installing one program, but because they fail to read the EULA, and the software attempts to hide itself in other

found insufficient to provide notice of hidden software that eroded consumers' privacy in an unexpected manner, typically serving pop-up advertisements, collecting information about consumer's on-line "clicks", or engaging in another insidious data collection technique. Through its spyware work, the Commission broadened the range of practices that trigger privacy concerns to include software that collects and transmits information about users, their computers, or their use of the content in addition to information that is narrowly considered personally identifiable, and signaled that the existence of formalities that might establish consent in contract law[128] would not preclude the Commission's inquiry into the sufficiency of notice and consent where consumer privacy is concerned.[129] The spyware cases also established the principle that some practices were so at odds with consumer expectations that regardless of the consent experience, they were actionable.

FTC actions against companies failing to prevent the breach of personal information similarly abandoned a legalistic, notice-bound analysis. In these actions, the Commission brought unfairness claims against companies that had not made representations regarding data security.[130] While these cases have settled quickly, the resulting consent decrees have established that the failure to employ certain security processes and practices, such as addressing commonly known and well-understood security vulnerabilities and identifying and preventing security vulnerabilities that put customer information at risk, constitutes unfairness. Specifically, firms feel compelled to employ practices and procedures that provide a "reasonable" level of security to protect

---

ways, they fail to understand that they are in fact installing several different software programs and often creating relationships with several different companies. Typically these programs engage in invasive activities (pop-up or other forms of push advertising) or extractive activities (monitoring and data collection) which users presumably would avoid if given appropriate notice. *In re* Advertising.com, USFTC File No. 042-3196 (Sept. 12, 2005) (holding failure to clearly and conspicuously disclose bundled software that traced browsing deceptive); *See also* Complaint, FTC v. Odysseus Mktg., Inc., No. 05-CV-330 (D.N.H. Sept. 21, 2005) (holding that failure to clearly and conspicuously disclose bundled software with security and privacy risks is deceptive).

[128] See Deirdre K. Mulligan and Aaron K. Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 22 BERK. TECH. L. J. 1157, 1205-1211 (2007).

[129] For example, the order in the Sony BMG matter requires that the installation of software from a CD, and the transfer of information by such software, requires heightened "clear and prominent" notice and consent, Sony BMG Consent Decree (prohibiting downloads unless a consumer "dictates his/her assent to install such software by clicking on a button or link that is clearly labeled or otherwise clearly represented to convey that it will activate the installation, or by taking a substantially similar action").

[130] For example see, In re BJ's Wholesale Club, Docket No. C-4148, Decision and Order § I, available at http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf; In re DSW, Inc., Docket No. C-4157, Decision and Order, available at http://www.ftc.gov/os/caselist/0523096/0523096c4157DSCDecisionandOrder.pdf; and In re CardSystems Solutions, Inc., Docket No. C-4168, Complaint (Sept. 8, 2006), available at http://www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf.

users' personal information,[131] employing a legal standard that is notoriously fluid, responsive to market context (in terms of threats and mitigations), and open to change, evolution, and reinterpretation.

The ambiguity as to what privacy protection requires of corporations developed through FTC practice mirrors the sense the ambiguity articulated by the interviewed privacy leaders. It is easy to understand why these leaders believe that "privacy" requires "looking around corners" to anticipate ways in which new technologies, and new practices comport with consumer expectations regarding information usage. The agency's move to flexible standards, and away from data protection rules, has let loose a renewed conversation about privacy issues –whether unique identifiers and IP addresses warrant protection as personal information, whether behavioral tracking raises novel privacy questions, what security practices firms must have in place—and what firms must do to treat consumers fairly—meet their expectations—in the electronic marketplace.

2. State Data Breach Notification Laws and the Harnessing of Market Reputation

If the FTC sought, through a variety of "soft" and "hard" regulatory approaches, to publicize the risks posed by emergent technologies and market practices on the one hand, and link legal standards to the vindication of consumer expectations on the other, the passage of state data breach notification laws provided a single concrete mechanism for strengthening the link between privacy protection and consumer trust. As discussed earlier,[132] these laws—of which 45 have been enacted since 2002—require corporations to notify individuals whose personal information has been breached, in an effort to tie corporate privacy performance directly to reputation capital.

The breach notification laws embody a governance approach that emphasizes "informational regulation," or "regulation by disclosure."[133] Such tools require the disclosure of information about harms or risks as a means of "fortify[ing]" either "political checks on private behavior" or "market mechanisms."[134] In this case, disclosure requirements seek to prompt both—and while disclosures have provided important

---

[131] *See* MTS Inc., 69 Fed. Reg. 23,205 (Fed. Trade Comm'n Apr. 28, 2004) (proposed consent order) (failure to implement procedures that were reasonable and appropriate to detect and prevent "broken account and session management" vulnerabilities was unfair or deceptive given Tower Records's statements about attention to security and privacy); Eli Lilly & Co., 67 Fed. Reg. 4,963 (Fed. Trade Comm'n Feb. 1, 2002) (proposed consent order) (lack of proper controls to avoid disclosure of email addresses was unfair or deceptive given statements to the contrary).

[132] *See infra*, text at notes __-__.

[133] Cass R. Sunstein, *Informational Regulation and Informational Standing:* Akins *and Beyond*, 147 U. PA. L. REV. 613, 613 (1999) (describing the shift to such an approach as "one of the most striking developments in the last generation of American law").

[134] *Id.* at 614.

factual predicates for FTC enforcement, they have also subjected privacy outcomes to market and consumer discipline in important ways.

The breach notification laws transformed previously unnoticeable corporate lapses into press events with deep implications for brand. While the extent to which companies notified affected individuals of a security breach that exposed personal information prior to the advent of the security breach laws is unclear, and difficult to assess systematically, very few press stories predating their enactment mention customer notification of breaches,[135] and both survey and anecdotal evidence (along with the fact that industry groups strongly objected to notification requirements on cost grounds)[136], support the conclusion that the security breach laws drove consumer notification well beyond prior practice in industry.

The notices moreover, have permitted privacy advocates to exploit media coverage in ways that keep public conversations about privacy and data protection on the front burner. Thus the Privacy Rights Clearinghouse maintains a chronology of data breaches, [137] while U.S. PIRG and Consumers Union have leveraged the steady drumbeat of security breaches to build momentum for the proliferation of model laws across states.[138]

By these mechanisms, in the words of one respondent, notification laws lead corporations to "[t]ry to avoid the breaches and the problems and the brand tarnishment issues and promote the ability to use and flow data in a proper way and make it a competitive advantage . . . ." While reported security breaches involving personal information result in both an immediate short-term impact on firms' stock price,[139] and direct remediation and litigation costs[140]—recently calculated at $197 per record breached[141]—the bulk of the penalty to firms arises from lost business, a phenomena that has nearly doubled between 2005 and 2007.[142] Lost business represents the costs related to customer "churn," or turnover, as well as increased costs of customer acquisition. These costs directly reflect consumer pushback arising from perceived failures in the

---

[135] *But see, e.g.*, *Travel Web Site Admits To Security Breach*, USA TODAY (Jan. 24, 2001) (describing Travelocity's email notification sent to 45,000 affected customers); Sarah Left, *Web Security Breach Forces Users To Cancel Cards*, THE GUARDIAN (June 22, 2001) (describing notice to 27,000 customers of exposure of credit card and other personal details).

[136] Jaikumar Vijayan, *Consumer Groups Rail Against Proposed Data-Breach Notification Law*, COMPUTERWORLD (March, 16, 2006) (discussing industry efforts to pass less stringent laws).

[137] http://www.privacyrights.org/ar/ChronDataBreaches.htm

[138] http://www.uspirg.org/financial-privacy-security/identity-theft-protection

[139] *See* Alessandro Acquisti, *et al.*, *Is There a Cost to Privacy Breaches? An Event Study*, Proceedings of the International Conference of Information Systems (ICIS) (2006) (discussing an impact of short duration, a 0.6% reduction in stock price on the day the breach is reported).

[140] *See* Joris Evers, *Break-in Costs Choicepoint Millions*, CNET NEWS (July 20, 2005).

[141] Larry Ponemon, 2007 Annual Study: U.S. Cost of a Data Breach Understanding Financial Impact, Customer Turnover, and Preventative Solutions (2007)

[142] See id.

protection of personal information, and directly affect the way in which privacy failures undermine trust and brand. But for the notification requirements of the law, it is highly unlikely that customers would have knowledge of the breach and place market pressure on companies to improve security practices. The consumer expectation rubric revealed in our interviews thus reflects an increasing reality prompted by the security breach disclosure laws and which in turn resonates with an evolving conversation linking trust, brand image and privacy.

Finally, the SBN laws created an incentive structure that drove companies to develop internal processes to manage risk.[143] The laws provided CPOs with a powerful performance metric, both internally and with respect to peer institutions. The CPOs we interviewed reported summarizing news reports from breaches at other organizations and circulating them to staff with "lessons learned" from each incident, and explained that that breaches at other organizations help justify expenditures for implementing new protocols within their own organizations. In the words of one respondent, "the breach news . . . was so loud that it didn't take much to get the attention of our senior executive on data security, kind of as part of the privacy program." Another reported, "[the security breach laws] enriched my role; it's putting more of an emphasis on leadership internally in a very operational sense." The visibility of privacy failures thus enhanced internal resources; as one CPO described, "we're now in the process of rolling encryption across all of our laptops. It's the right thing to do and I'm very glad we're doing it but, if it wasn't for the security breach laws in the U.S., we wouldn't be doing it. I don't think any company would be. It's what drove it."

D. The Turn to Professionals

While the rhetoric of privacy as trust was no doubt appealing to corporate privacy officers trying to gain traction within their organizations—as it was for regulators attempting to motivate industry to take privacy seriously or face a barrier to electronic commerce—the combination of uncertainty as to the FTC's evolution of privacy requirements, and as to market responses spurred by data breach notifications was central to the striking trend towards corporate reliance on professional privacy management described in Section 2.B.

Professionalism has long served as an important institution for mediating uncertainty in the face of environmental ambiguity,[144] And in the privacy context,

---

[143] *See also* Deirdre K. Mulligan & Joseph Simitian, "Security Breach Notification Laws: A Race to the Top?" (unpublished manuscript on file with the authors) (identifying similar impact of SBN laws in areas such as asset management, portable media encryption and the development of best pratices).

[144] *See generally*, Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*. 53 AM. ECON. REV. 941, 947 (1963) (describing how physician professionalism was an intermediating "nonmarket social institution" that compensated for uncertainty in the context of the severe information asymmetry between market actors); Lauren B. Edelman, *Legal Ambiguity and Symbolic Strustures: Organizational Mediation of Civil Rights Law*, 97 AM. J. SOCIOL. 1531 (1992) (discussing the importance of professionals in mediating legal ambiguity within organizations).

increasing ambiguity as to the future behavior of both regulators and market forces prompted a parallel escalation in the reliance on internal corporate experts, grounded in knowledge and experience of privacy regulation's trajectory, to guide corporate practices and manage privacy risk.

Our interviews reflect this risk-management orientation by their forward-looking focus on identifying future challenges, rather than on compliance with existing mandates. They also underscore the potential for environmental ambiguity, combined with credible threats of meaningful sanction, in affecting the scope of the privacy function within corporate organizations; our respondents described a broad reach throughout the corporation, authority to participate in strategic decisions about the firm business, and a relatively wide latitude to establish corporate practices and define their jobs. In words attributed to one corporate employer: "we want to have a wonderful privacy program and you tell us what that means."

IV. THE IMPLICATIONS FOR POLICY DEBATES

By this account of privacy "on the ground," the dramatic rise in corporate resources and attention accorded privacy management since 1998, and its development of privacy frameworks to guide decisionmaking in new contexts, tracks a transformation of the privacy field more generally. While the dominant account of U.S. privacy regulation—of privacy "on the books"—correctly argues that U.S. law fails to provide the robust FIPPS protections and comprehensive rule- and enforcement- structures developed in Europe, the alternative account illuminates the concurrent entry of a new force into the regulatory space—the Federal Trade Commission—and the way in which its activities, together with the involvement of advocates, professionals, and market forces, framed a new discourse regarding privacy protection. Far from reducing uncertainty in the legal field, that agency's "soft" regulatory tools and "roving" exercise of enforcement power increased legal ambiguity. But in doing so, they contributed to the augmentation of the discourse around privacy from one focused on procedural mandates to one that includes a substantive measure: the vindication of consumer expectations regarding the treatment of personal information.

Grounding the debate over the U.S. privacy-protection framework has deep implications for public policy, at a time that the Obama Administration and Congress are considering an overhaul of federal privacy statutes, and the OECD reconsiders global privacy approaches on the occasion of the thirtieth anniversary of its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[145].

These implications, first, touch debates over how privacy is framed. We have no truck with those who argue for strengthening procedural methods of protecting personal information. Yet the grounded account of privacy casts into relief the incompleteness of

---

[145] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*', *Organisation for Economic Cooperation and Development*, (1980).

a reliance on formal notice, consent and information alone to protect against real harms as rapid technology changes reduce the power of individuals to isolate and identify the use of data that concerns them. It suggests the frailty of a procedural understanding of privacy protection in guiding corporate decisionmakers, *ex ante*, in making choices about the technologies they employ in products or processes. And it indicates that a combination of field participants have refocused on a substantive approach of privacy protection that important theorists suggest best vindicate individual and societal interests: one that emphasizes objective expectations over subjective formalism, dynamism in the face of technological and advance, and application by context.

Moreover, the account of privacy on the ground offers important lessons for debates over regulatory form. While traditional regulation eschewed uncertainty in favor of regulatory specificity, more recent governance approaches increasingly experiment with ambiguous mandates, "delegating" to regulated parties greater discretion in fulfilling legal goals.[146] Nonetheless, such regimes can produce merely "symbolic" or "cosmetic" self-regulation, as participants in the legal field shape understandings of conformity that undermine or contort the public goals they purport to advance. The account of privacy on the ground, however, describes a regulator's deployment of a broad legal mandate by means of a suite of "New Governance" approaches—measurement, publicity, learning, dialogue, and process, as well as credible, yet indeterminate and evolving, threats of enforcement—in a way that centered the public voice in shaping both the law's framing and the "compliance-plus" mindset reflected by the interviewed privacy leaders. In this context, the account suggests, a substantive approach to privacy, increased executive attention, and the corporate privacy management's move from the legal compliance office into product and business decisions arose because, rather than in spite, of regulatory ambiguity.

A. Implications for the Substantive Debate Over Privacy Regulation

The emergence of consumer expectations as a measure with which to judge privacy protection introduces an independent overlay to a legal framework that otherwise relied on the formal satisfaction procedural indicia of consent. In framing privacy's meaning and what values it serves, this new measure adds a rubric rooted in substantive norms, social values, and evolving community practice, to existing approaches emphasizing procedural tools, individual autonomy, and personal choice.

This overlay does not deny the value of formal notice, information, and consent protections; rather, it eliminates the presumption that the existence of procedural mechanisms are conclusive of an interaction's fairness. Thus while the FTC's early actions focused on enforcing the bargains between individuals and corporations—regardless of their content—later actions found certain practices to be unreasonable regardless of individual "consent" by means of the standard click-wrap processes generally upheld by courts. Unfairness and deception concern whether a practice,

---

[146] See Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377, 377 (2006).

including the notice that accompanies it, falls outside some acceptable level of deviation from, past consumer experience. Those inquiries rely on understandings that consumers bring to an transaction—the "mental model" they have of information "flows?"—and whether a practice is unexpected in light of those understandings, and therefore violative of public policy. As a conceptual matter, a notion of privacy as a public policy or social value is superimposed over existing notions of its link to individual autonomy. As a practical matter, new or unanticipated information flows will trigger legal scrutiny.[147]

By diversifying legal understandings of privacy,[148] then, the development of the consumer expectations rubric provides an additional protection framework that scholars from diverse fields suggest can provide a more robust conception of privacy values deserving of defense; a framework that offers a means to identify privacy problems *ex ante* in contexts that procedural protections cannot; a framework that is not reflected FIPPS principles.

As these scholars explore, defining privacy as "informational self-determination" at once claims too much, and protects too little. By its emphasis on choice, this definition recognizes that privacy's requirements can vary by context; for example, information will be appropriate to share in some contexts, with some recipients, and for some purposes—but not others. Yet the notion that law should provide individuals with a common set of mechanisms for vindicating privacy, the animating principle behind the push for "omnibus" regulations, requires that "information privacy policy [be] based inevitably . . . on procedural, rather than substantive, tenets," by which "individuals can assert their own privacy interests and claims if they so wish," and "the content of privacy rights and interests have to be defined by individuals themselves."[149] As such, the substantive interest in the protection of privacy values is transformed into a "right" to procedure.

Even on its own terms, this procedural definition places prohibitive costs, and unrealistic expectations, on privacy's actualization. One recent study demonstrated that an average person would expend between 91 to 293 hours per year were they to skim the privacy policy at each website visited, and 181 to 304 hours if they actually read them.[150] . In real terms, then, even the procedural right is often an empty one.

---

[147] This formulation of privacy bears some semblance to the two-part test used in Fourth Amendment cases. *See* Katz v. United States, 389 U.S. 347 (1967). However, unlike that jurisprudence's "reasonable expectations" test, under which the very existence of new surveillance and data-collection technologies generally eroded the sphere of reasonable expectations, the FTC's formulation is protective in its bias—the expansion of surveillance and information-collection capacity in new ways is understood to signal unanticipated information flows and the loss of privacy that may flow from them.

[148] *See* DANIEL SOLOVE UNDERSTANDING PRIVACY 187 (2008) (discussing the "Benefits of a Pluralistic Understanding of Privacy").

[149] COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 9 (2006).

[150] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. OF L. & P. FOR THE INFO. SOC., (2008) (the ranges reflect the low, point and high estimates they arrived at through study for skimming and reading policies). The study ultimately concludes that reading

More generally, the mindset of data-protection through procedural mechanisms is mismatched to paradigm changes in the technology landscape; it is "not quite able to conform to the ebb and flow of anxieties that these systems and practices provoke."[151] Framing privacy protection as mechanisms facilitating discrete decisions regarding access to or acquisition of data places the substantiation of privacy's meaning in an individual's hands at one particular time, without knowledge or foresight about the changes in information treatment that future technologies and practices will bring.

This framing, moreover often provides no "decision heuristic,"[152] no substantive touchstone, to guide the choices of those with far greater power to shape privacy's treatment: corporate actors shaping the systemic decisions about design choices that impact information usage. Most simply, decisions at the corporate level might provide the best way to avoid privacy harms.[153] But perhaps more pervasively, providing a substantive metric to guide such systemic decisions recognizes the fact that the values embedded in technology systems and practices shape the range of privacy-protective choices individuals can, and do, make regarding interactions with those systems and practices.[154] Technology can both be shaped and shaped by, social context.[155] An abdication of the opportunity to provide a substantive decision heuristic for technology shapers, therefore, permits other interests to limit the very choices that a "self-determination" emphasis suggests must be accorded to individuals.

The failure of "information self-determination" as a heuristic for corporate decisionmaking was emphasized in the comments from those chief privacy officers considering contexts characterized by the greatest technological change.[156] When

---

privacy policies costs approximately 201 hours a year at a vlue of $3,534 annually per American Internet user, or about $781 billion annually for the nation).

[151] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE 148 (2010). This is reflected the fears of scholars and advocates who find that data protection can lead to a reductive construction of privacy and therefore resist working "within any fixed and guiding definition of what privacy means," COLIN BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE 18 (2008).

[152] NISSENBAUM, *supra* note __ at 148.

[153] *See generally*, GUIDO CALABRESI, THE COST OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS (1970). (adopting Coasean insights regarding assigning liability to promote decisionmaking by the "cheapest cost avoider," and therefore the party best able to avoid harms).

[154] *See* Martin Heidegger, *The Question Concerning Technology*, *in* TECHNOLOGY AND VALUES: ESSENTIAL READINGS 99, 106–08 (Craig Hanks ed., 2010) (describing the way technology shapes a *Gestell*, or world view, that alters the perceptions of the decisionmakers it informs); *see generally* LAWRENCE LESSIG, CODE VERSION 2.0, at 5 (2006) (describing the regulatory power of "code"); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEXAS L. REV. 553, 554 (1998) (discussing the regulatory power of technological capabilities and system design choices).

[155] *See* Patrick Feng, *Rethinking Technology, Revitalizing Ethics: Overcoming Barriers to Ethical Design*, 6 SCI. & ENGINEERING ETHICS 207, 211–12 (2000) (describing the Science and Technology Studies insight that "technology both shapes and is shaped by its social context" (emphasis omitted)).

[156] *See supra*, text at nn. __-__.

dealing with business practices involving constant connectivity such as ubiquitous computing, in which information is sensed and exchanged as part of the product offering, or health technologies whose value derives explicitly from "get[ting] in the body," privacy must inform contextual, changing, and nuanced decisions about the very structure of the service provided, and procedural mechanisms are of limited use. In these contexts they have sought normative guidance from the evolving metric of consumer expectations.[157]

Philosopher and theorist Helen Nissenbaum describes the ways in which norms informed by social expectations can provide a far more robustly-protective frame for privacy than its definition as a set of one-off individual choices. The latter, she describes, encourages the mistakes of "moral mathematics" described by philosopher Derek Parfit.[158] A focus on informational "self-determination" limits the balance involved in privacy choices to the costs and benefits accruing to an individual decisionmaker. It thus precludes inquiry as to whether "my act [will] be one of a set of acts that will *together* harm other people,"[159]—and therefore ignores privacy's importance as a social good.

Nissenbaum explores the socially-situated nature of privacy, arising from the reality that "we act and transact not simply as individuals in an undifferentiated social world, but as individuals acting and transacting in certain capacities as we move through, in, and out of a plurality of distinct social contexts." [160] Each of these social contexts is governed by a set of norms derived from history, culture, law and practice. Such norms "govern key aspects such as roles, expectations, behaviors, and limits" in any given situation. They also provide two types of informational norms important to understandings of privacy: norms of information appropriateness and distribution. Norms of "appropriateness,"

> dictate what information about persons is appropriate, or fitting, to reveal in a particular context. Generally, these norms circumscribe the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed.[161]

---

[157] Privacy scholar Priscilla Regan has documented, moreover, the ways in which internal corporate debates on privacy are more responsive to an available language of privacy as an enabler of some other collective social good, as opposed to as an individual right, *see* REGAN, LEGISLATING PRIVACY (1995).

[158] *See* NISSENBAUM, *supra* note _ at 242 (quoting DEREK PARFITT, REASONS AND PERSONS 86 (1986)).

[159] *Id.*; *see also generally*, Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 959 (1989) (offering a normative account of privacy that does not focus just on the protection of individuals, but also on protection of the community, and finding that privacy torts in the common law uphold social norms, which in turn contribute to both community and individual identity).

[160] *See* NISSENBAUM, *supra* note _ at 129.

[161] *Id.* at 140.

Norms of distribution, by extension, examine "whether [the information's] distribution, or *flow*" is consistent with context specific norms ranging from expectations of confidentiality and discretion to entitlement and obligation to reuse or re-disseminate.[162] Thus, as Robert Post has described, privacy norms "rest not upon a perceived opposition between persons and social life, but rather upon their interdependence."[163]

These norms vary by context and evolve over time, but at any one point embody the situational clues and understandings that inform individual cognition,[164] permitting efficient decisionmaking by precluding the need for individuals to engage in the impossible task of collecting and assessing all information anew.[165] From here derives the social value of expectations: when these understandings are upended, each of the participants in a social context will be deprived of accurate inputs for their decisions, resulting in unintended and unexpected, breaches in "contextual integrity,"[166] and therefore their privacy.[167]

The privacy-protective power of a substantive consumer expectations overlay onto procedural protections is reflected by a host of recent incidents in the privacy domain.

In some, expectations have provided a basis for fortifying notice and consent procedures themselves. The FTC's recent consent order with Sears Holding

---

[162] *Id*.

[163] Post, *supra* note __ at 959.

[164] *See generally* Mark C. Suchman, *On Beyond Interest: Rational, Normative and Cognitive Perspectives in the Social Scientific Study of Law*, 1997 WIS. L. REV. 475, 483 (describing the normative perspective on decisionmaking, which emphasize the selection of the norm that applies by first identifying the context as one in which the norm should prevail).

[165] "The capacity of the human mind for formulating and solving complex problems is very small compared with the size of the problems whose solution is required for objectively rational behavior in the real world," HERBERT A. SIMON, MODELS OF MAN 198 (1957) (emphasis omitted). "The human mind adapts to these shortcomings by developing unconscious cognitive shortcuts that generally make it easier to make sense of new situations even in the absence of complete information," Bamberger, *Regulation as Delegation*, *supra* note __ at 411. Thus rather than "maximizing," their choices, humans consider only a few possible courses of action and "satisfice[]," HERBERT A. SIMON, ADMINISTRATIVE BEHAVIOR xxix (3d ed. 1976), choosing to settle for a solution that is adequate.

[166] See Nissenbaum, supra note __ at 158-185.

[167] This focus on privacy as a social good finds resonance in the privacy advocacy community as well. While many advocates frame privacy in the context of protecting individual rights, others emphasize its value to society in limiting abuses by those with power, *see* COLIN BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE, 20-23 (2008). For these advocates the focus on data protection distracts from conversations about the responsibility of corporations to consider the privacy and human rights impacts of the technology they build, and services they offer, *see generally* John G. Palfrey, *Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet*, GLOBAL INFO. TECH. REP., 69 (2006); *Website*, Global Network Initiative http://www.globalnetworkinitiative.org/

Management Corporation,[168] for example, targets the company's use of an email invitation to join their "MY SHC Community" and download a program that ran in the background on users' computers and transmitted information on virtually all of the users' Internet use to Sears, including web browsing, business transactions during secure sessions, completing online application forms, checking online accounts, and use of web-based email and instant messaging services—pushing against Nissenbaum's "appropriateness" norm. Specifically, it challenges the company's communications with users, which explained that "[t]his research software will confidentially track your online browsing," and only disclosed all the details about the function of its tracking software in a separate scrollbox. The scrollbox and standard click-through agreement used were of the kind generally upheld by courts. But the FTC decided that a detailed understanding of these unexpected practices reached such a level of materiality for consumers that it must be made "unavoidable" in consumer transactions.

Similar notions animate the response to practices surrounding the launch of Google's new social networking service, Buzz. That service's default options led, for many consumers, to the unexpected public disclosure—implicating Nissenbaum's distribution norm[169]—of the list of the people they email and chat with most frequently (including journalists' sources and therapists' patients). Rejecting outright the claims that formalities had satisfied privacy mandates, advocates and critics have both framed the nature of the violations, and rooted solutions, squarely in the language of expectations. Thus CNET's Molly Wood critiques,

> But I *do* have an expectation of privacy when it comes to my e-mail, and I think that even in this age of social-networking TMI, most people still think of e-mail as a safe place for speaking privately with friends and family. And for Google to come along and broadcast that network to the world without asking first—and force you to turn it off after the fact—is, I think, both shocking and unacceptable.[170]

In turn, writes Kurt Opsahl of the Electronic Frontier Foundation, the problem is that Google "failed to provide users with the setting users had reasonably expected."[171] Thus the appropriate privacy-protective behavior: "mak[ing] secondary uses of information

---

[168] In the Matter of Sears Holdings Management, File No. 082 3099 (FTC), *available at* http://www.ftc.gov/os/caselist/0823099/index.shtm

[169] *See e.g.*, Complaint of the Electronic Privacy Information Center, In the Matter of Google, Inc., ¶ 8, *available at* http://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf ("While email senders and recipients always have an opportunity to disclose email-related information to third parties, email service providers have a particular responsibility to safeguard the personal information that subscribers provide.")

[170] Molly Wood, *Google Buzz: Privacy Nightmare*, CNET NEWS (Feb. 10, 2010), *available at* http://news.cnet.com/8301-31322_3-10451428-256.html.

[171] Kurt Opsahl, *Google's "Buzz" Should Have Required Consent For Secondary Use Of Private Information*, JURIST (Feb. 24, 2010) (commentary by Electronic Frontier Foundation senior staff attorney).

only with clear, unequivocal user consent and control, and test these controls to ensure that the default settings match with the expectations of the user."[172]

In other contexts, a consumer expectations framework has been used to protect privacy where technological changes render traditional reliance on consent inoperative. In light of advances in capacity permitting data storage for far longer periods than ever expected, for example, a recently released FTC staff report on behavioral advertising stated that, companies may "retain data only as long as is necessary to fulfill a legitimate business or law enforcement need"[173]—thereby removing data retention time frames from the private bargaining between individuals and corporations in the marketplace.

Finally, expectations provide a measure for privacy protection even in circumstances in which procedural protections are inapposite. An early example involves Intel's decision to attach a unique serial number to each Pentium chip. Considered against a background of a proliferation of device and application identifiers, the FIPPS principles had offered no indication that a serial number on a chip would raise a privacy uproar, or would trigger the need for procedural requirements. The Pentium serial number was not tied in any way to the type of personally identifiable information that at that time was typically the trigger for FIPPS requirements. Yet advocates singled the PSN out for the ease with which the number could be remotely and invisibly requested, and the possibility that the unique identifier would be used to track the actions of a computer across the internet. Because of Intel's market penetration and position in the internet ecosystem, and the ease with which even anonymized behavioral data can be used to detect individual identity,[174] the company had essentially embedded a tracking device in each computer—or in the colorful words of one advocate "branded (it) with an identifier."[175] If procedural protections could not address this concern, substantive encroachment on consumers' normative understandings did, leading to an FTC complaint, a call for a boycott, and advocate-generated pressure from computer manufacturers.[176]

B. Implications for Debates over Regulatory Form

---

[172] *Id.*

[173] FTC, Staff Report: Self-Regulatory Principles for Online Behavioral Advertising 47 (Feb. 2009).

[174] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. (forthcoming 2010) (manuscript at 42–43, on file at http://ssrn.com/abstract=1450006) (discussing anonymization's failure to preclude reidentification techniques).

[175] Declan McCullagh, *Intel Nixes Chip-Tracking ID*, WIRED (Apr. 27, 2000) (quoting David Sobel, General Counsel, Electronic Privacy Information Center).

[176] The Center for Democracy and Technology asked equipment manufacturers (OEMs) for information about how the PSN would be implemented in their devices. Several responded indicating that they would provide users with greater control. For the history see http://opt-out.cdt.org/privacy/issues/pentium3/ ; for the letter to OEMs see http://opt-out.cdt.org/privacy/issues/pentium3/990216oem.letter.shtml for OEM default settings see http://opt-out.cdt.org/privacy/issues/pentium3/990414OEM.shtml

As much as the account of privacy on the ground can inform disputes over regulation's content, it also offers profound implications for debates over its form. Specifically, it provides important perspectives on questions regarding the optimal specificity of regulatory mandates regarding privacy, and regarding the institutional structures of privacy governance.

1. Debates Over Regulatory Specificity and Ambiguity

Traditional command-and-control regulation seeks to achieve particular outcomes by articulating, *ex ante*, uniform rules requiring certain conduct. Such a rules-based approach reflects faith in regulatory entities to be able to determine, in a top-down manner, the best means for achieving regulatory goals. Its emphasis on regulatory specificity permits little compliance discretion; regulated parties can either comply with requirements, or fail to do so. Moreover, the more "complete" the codification of behaviors, the more it anticipates possible contingencies, and direct behaviors accordingly.[177]

The shortcomings of command-and-control governance, however, are well recognized.[178] Rules are notoriously both under-and over-inclusive, identifying certain relevant factors that can easily be codified, while ignoring others. Specific rules often cannot reflect the large number of variables involved in achieving multifaceted regulatory goals, such as reducing the types of risk produced by a combination of factors.[179] And specific commands reflect, in a static manner, their authors' beliefs about the best way to achieve general principles at the time of promulgation; as a tool, codified rules lack the agility to adapt to changing circumstances and new understandings.

For these reasons, reliance on compliance with a set of detailed provisions may frustrate, rather than further, underlying regulatory ends. Rule systems are inevitably incomplete, failing to provide guidance in a host of contexts, especially as circumstances change. At the same time, they can have detrimental effects on decisions within the organizations they govern, leading to a process of bureaucratization that results in "goal displacement," by which compliance with partial but specific rules—originally promulgated as a means for achieving a regulatory goal—becomes the singular end.[180] In particular, a bureaucratic "compliance"-oriented approach, by which rules of action are communicated in a centralized top-down fashion and intended to be applied by others

---

[177] *See generally*, JEREMY BENTHAM, A GENERAL VIEW OF A COMPLETE CODE OF LAWS (1802) (presenting the ideal of a "complete code").

[178] *See, e.g.*, Cass Sunstein, *Administrative Substance*, 40 DUKE L.J. 607, 627 (1991) (citing failures in using "rigid, highly bureaucratized 'command-and-control' regulation" to govern "hundreds, thousands, or even millions of companies and individuals in an exceptionally diverse nation").

[179] *See, e.g.*, Susan Sturm, *Second Generation Employment Discrimination: A Structural Approach*, 101 COLUM. L. REV. 458, 461 (2001) (discussing the problems with regulating the "complex and dynamic problems inherent" in workplace bias with "specific, across-the-board rules").

[180] *See generally* ROBERT K. MERTON, SOCIAL THEORY AND SOCIAL STRUCTURE 195-206 (1957) (discussing the process of "goal displacement," whereby "an instrumental value becomes a terminal value").

with little contextual knowledge, can disempower those within organizations who are charged with carrying out policies,[181] constraining internal pressures for greater resources and attention. It can alienate them from the goals behind the rules in favor of a focus on formalism, which in turn leads to a routinization of decision processes[182] that results in a greater number of human error events when implementing external regulation.[183]

The extensive literature on the economics of contracts identifies such problems with "complete" contracting—attempting to fully articulate terms *ex ante*—in situations of complexity and uncertainty.[184] In such circumstances, an instrument's terms should be left vague or unspecified, while assigning future decisions about how to resolve imprecision to parties that will, at the appropriate time, have best access to relevant information.[185]

These insights have shaped choices about regulatory design. Indeed, the past two decades have seen widespread experimentation with regulatory requirements framed in terms of broad principles rather than precise rules, and therefore that create greater ambiguity regarding appropriate methods of compliance.[186] In contexts as diverse as securities regulation, employment discrimination, and domestic terror protection,[187] policymakers have turned increasingly to general mandates rather than specific requirements in an attempt to deal with the complexity of the public goals at issue.[188]

---

[181] See Alfred A. Marcus, Implementing Externally Induced Innovations: A Comparison of Rule-Bound and Autonomous Approaches, 31 ACAD. OF MGM'T J. 235 (1988).

[182] *See* Bamberger, *Regulation as Delegation*, *supra* note __, at 445 (discussing studies indicating that making monitoring criteria well-specified and known to decisionmakers "exacerbates the substitution of cognitive shortcuts for reasoned judgment, and promotes routinized 'check the box' compliance").

[183] See Marcus, supra note __ at 235.

[184] *See generally* Robert E. Scott & George G. Triantis, *Incomplete Contracts and the Theory of Contract Design*, 56 CASE W. L. REV. 187, 191 (2005) ("In contract theory, incompleteness is due to the fact that information is costly and sometimes unavailable to (a) the parties at the time of contracting or (b) the parties or the enforcing court at the time of enforcement.").

[185] *See generally* OLIVER E. WILLIAMSON, THE ECONOMIC INSTITUTIONS OF CAPITALISM: FIRMS, MARKETS, RELATIONAL CONTRACTING 34 (1985) (discussing "governance structures" put into place to resolve future contractual uncertainty).

[186] *See* Cristie L. Ford, *New Governance, Compliance, and Principles-Based Securities Regulation*, 45 AM. BUS. L. J. 1, 5 (2008) (contrasting principles-based regulation with "the more prescriptive and inflexible mechanisms associated with classical regulation"); Bamberger, *Regulation as Delegation*, *supra* note __ at 390-392 (discussing the increased reliance on regulation that "articulates general goals," yet "make[s] few *ex ante* decisions about substantive detail").

[187] *See* Ford, *supra* note __ at 1; Sturm, *supra* note __ at 461; Kenneth A. Bamberger, *Global Terror, Private Infrastructure, and Domestic Governance*, in 2 THE IMPACT OF GLOBALIZATION ON THE UNITED STATES: LAW AND GOVERNANCE 204 (2008).

[188] *See* Bamberger, *Regulation as Delegation*, *supra* note __ at 386-392 (discussing "The Trend Towards Regulatory Delegation").

This development has provided regulators with important tools for overcoming the challenges they face in identifying either threats on the ground or private information about firm organization necessary for developing uniform top-down requirements for risk-mitigating behavior.[189] Framing legal mandates broadly leaves space for discretion in implementation. By permitting heterogeneous and flexible methods of compliance in individual firm contexts, such framing provides a means for enlisting the judgment of firm decisionmakers, drawing on their superior knowledge both about the ways risks manifest themselves in individual firm behaviors and business lines, and about available risk-management capacities and processes.[190] It further accords regulators continuing flexibility in the face of uncertainty as to how public goals should be furthered in diverse and heterogeneous contexts, and quickly shifting landscapes over time.[191]

Yet scholars have also questioned the reliance on ambiguity as to the meaning of legal mandates as a regulatory tactic, pointing to numerous contexts suggesting this method's failure in achieving public goals. Most simply, eschewing specific top-down commands can render regulation hollow; regulated firms are freed from compliance with concrete measures, while resource constraints, industry pressure, and the complexity of the task, can derail regulators' efforts to give meaning to the broad language they are charged with enforcing. In these contexts firms are unrestrained both from incentives to expend effort in furthering public goals, and from the "external shocks" wrought by regulatory action and the credible threat of enforcement, the type of events that are frequently necessary to spur meaningful internal organizational change.[192]

Even when firms take compliance measures, scholars have argued, legal ambiguity can permit a form of evasive self-regulation. Specifically, the absence of specified requirements allows regulated firms to adopt practices that might appear to further the broad regulatory mandate, but are merely "cosmetic," in that they "do not deter prohibited conduct within firms and may largely serve a window-dressing function that provides both market legitimacy and reduced legal liability."[193]

---

[189] *See* Edward L. Rubin, *Images of Organizations and Consequences of Regulation*, 6 THEORETICAL INQUIRIES L. 347, 386 (2005) (describing fact that regulators often impose counterproductive measures because they lack knowledge of particular firms' internal operations).

190. *See* IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE 110–13 (1992) (describing the public and private benefits of an enforced self-regulation model, which takes advantage of the greater expertise and information of firm insiders).

[191] *See* generally, Vince Fon & Francisco Parisi, *On the Optimal Specificity of Legal Rules*, 3 J. INSTITUTIONAL ECON. 147, 147 (presenting a model of optimal specificity of laws suggesting the use of standards instead of rules in areas undergoing rapid change).

[192] See generally, Neil Fligstein, The Structural Transformation Of American Industry: An Institutional Account Of The Causes Of Diversification In The Largest Firms, 1919–1979, in THE NEW INSTITUTIONALISM IN ORGANIZATIONAL ANALYSIS (W. Powell and P. DiMaggio, eds), 311 (1991) (discussing how 'external shocks' provided by legal institutions, macroeconomic conditions, or other organizations can provoke change in an otherwise stable field).

[193] Kimberly D. Krawiec, Cosmetic Compliance and the Failure of Negotiated Governance, 81 WASH. U. L.Q. 487 (2003); see also generally Kenneth A. Bamberger, Technologies of Compliance: Risk and Regulation in a Digital Age, 88 TEX. L. REV. __ (2010) (discussing the ways in which

These critiques are deepened by the contributions of socio-legal scholars exploring the way that legal and organizational "fields"[194]—the constellation of organizational actors participating in a particular domain—construct legal meaning in the face of ambiguity. Faced with an unclear mandate, firms have strong incentives to adopt "ceremonial"[195] compliance measures, procedures sufficient to signal "legal legitimacy" while simultaneously limiting law's impact on managerial power," or otherwise disrupting central firm structures.[196] Such practices, in turn, spread to other firms, which mimic what are perceived to be "successful" compliance models.[197] In such a fashion, compliance responses are institutionalized and ambiguous law is given contours.

In the employment context, for example, Lauren Edelman and others have traced the construction of compliance with equal opportunity laws such as Title VII's instruction that "[i]t shall be an unlawful employment practice for an employer . . . otherwise to discriminate against any individual . . . because of such individual's race, color, religion, sex, or national origin"[198]—language that "is ambiguous both in a legal sense and with respect to organizational policy."[199] In concert with "weak enforcement

---

technology systems that firms use to comply with broad risk-management mandates can "permit individual actors motivated by organizational incentives and individual greed to manipulate their behavior in ways that mask [risk]"); Kimberly D. Krawiec, Organizational Misconduct: Beyond the Principal-Agent Model, 32 FLA. ST. U. L. REV. 571 (2005) (arguing that organizations have perverse incentives to implement ineffective compliance programs); Lawrence A. Cunningham, The Appeal And Limits Of Internal Controls To Fight Fraud, Terrorism, and Other Ills, 29 J. CORP. L. 267, 335 (explaining that an emphasis on corporate internal control systems put into place to signal regulatory compliance with broad mandates "can lead controls to take on the character of ends in themselves, rather than means of achieving ultimate goals").

[194] *See* Lauren B. Edelman, *Overlapping Fields and Constructed Legalities: The Endogeneity of Law*, IN JUSTIN O'BRIEN, ED., PRIVATE EQUITY, CORPORATE GOVERNANCE AND THE DYNAMICS OF CAPITAL MARKET REGULATION 58 (2007) (defining a legal field as "the environment within which legal institutions and legal actors interact and in which conceptions of legality and compliance evolve"); Paul J. DiMaggio & Walter W. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, 48 AM. SOC. REV. 147, 150 (1983) (defining an organizational field as "[t]hose organizations that, in the aggregate, constitute a recognized area of institutional life: key suppliers, resource and product consumers, regulatory agencies, and other organizations that produce similar services or products.").

[195] John W. Meyer & Brian Rowan, *Institutionalized Organizations: Formal Structure as Myth and Ceremony*, 83 AM. J. SOC. 340, 340–41 (1977).

[196] Shauhin A. Talesh, The Privatization of Public Legal Rights: How Manufacturers Construct the Meaning of Consumer Law, 43 L. & SOC. REV. 527, 533-34 (2009).

[197] New-institutionalist sociologists identify the process of three varieties of "isomorphism," by which understandings are diffused through an organizational field. "Mimetic" isomorphism, describes the process by which organizations respond to contexts in which goals are ambiguous and success difficult to measure by imitating others in the field who appear to be successful or legitimate, DiMaggio & Powell, *supra* note __ at 151-52.

[198] Title VII of the 1964 Civil Rights Act, section 703(a), 42 U.S.C. 2000e–2.

[199] Lauren B. Edelman, Legal Ambiguity and Symbolic Structures: Organizational Mediation

mechanisms" that provide "inadequate and inconsistent feedback on what organizational practices are legal," such laws thus leave regulated parties "wide latitude to construct the meaning of compliance."[200] In response, regulated organizations have focused compliance efforts on creating formal processes, including legalistic procedures for handling discrimination complaints. Such procedures appeal to legal norms by signaling an organization's "legality" but, because they are distinct from other firm structures, they can arise without the existence of fundamental alterations to existing workplace culture. These organizational responses to antidiscrimination law, in turn, spread throughout corporate practice, and were ultimately accorded deference by courts struggling for a metric to determine whether corporate practice satisfied the substance of the statute.[201]

By this process, the "right to a nondiscriminatory workplace in effect becomes a 'right' to complaint resolution."[202] Yet the right to complaint resolution "is far more superficial and entails fewer disruptions of routines than would a right to a nondiscriminatory workplace."[203] Legal meaning is resolved, but in a way that substitutes substance for process, and constrains law's effect. This phenomenon, moreover, track developments in a host of other contexts.[204]

2. Ambiguity in the Privacy Sphere

Debates over privacy regulation track these broader contests over regulatory form. Jeff Smith's study of privacy practices in 1994 concluded that the absence of clearly articulated legal aims and implementation strategies led to corporate inaction as CEOs avoided murky areas with unclear obligations and uncertain pay-off. "[T]he ambiguous corporate privacy domain," he concluded, was a primary driver of the "poor policy-making dynamic—the drift-external threat-reaction cycle"[205] in which firms avoided proactive privacy management, and executives only confronted privacy issues in face of specific, and limited, external threats. Ambiguity, moreover, was the condition "from which the other problems originate."[206] The trickle-down effect of a narrow focus only on compliance with specific mandates left employees charged with promoting privacy powerless to raise normative claims in tension with other organizational goals, leading to

---

of Civil Rights Law, 97 Am. J. Sociol. 1531, 1532 (1992).

[200] *Id*.

[201] Lauren B. Edelman, et al. Diversity Rhetoric and the Managerialization of Law, 106 AM. J. SOCIOL. 1589 (2001).

[202] Lauren B. Edelman et al., *Internal Dispute Resolution: The Transformation of Civil Rights in the Workplace*, 27 LAW & SOC'Y REV. 497, 529 (1993).

[203] Carol A. Heimer, *Explaining Variation in the Impact of Law: Organizations, Institutions, and Professions*, *in* 15 STUDIES IN LAW, POLITICS, AND SOCIETY 29, 41 (Austin Sarat & Susan S. Silbey eds., 1995).

[204] *See also*, *e.g.*, Talesh, *supra* note __ at 527 (describing a similar way in which "the content and meaning of California's consumer protection laws were shaped by automobile manufacturers, the very group these laws were designed to regulate.").

[205] SMITH, *supra* note __ at 167; *see generally id*. at ch. 6.

[206] *Id*.

an "emotional dissonance" that resulted in "redefining privacy"[207] in a manner that uniformly mitigated conflicts in favor of business profit. Contemporary critiques of privacy on the books echo these concerns, calling for greater specification of "command and control" privacy requirements across sector and practice.[208]

An account of privacy "on the ground," however, indicates otherwise. While in 1994 Smith viewed ambiguity as a "bug," this current account sees it as a "feature"—as a means for providing a space within which regulators could play an active role in catalyzing the privacy field's development of legal meaning that involved a variety of important institutional players, supplemented procedure with substantive heft, and has entailed far more robust, and more dynamic, corporate attention to privacy management.

A grounded account justifies the worries attendant to a singular reliance on highly-specified and proceduralized regulatory mandates. A recently–released multidisciplinary report reviewing the EU's Data Protection Directive, for example, finds that its focus on specific process rather than substantive outcomes "risks creating an organisational culture that focuses on meeting formalities to create paper regulatory compliance (via check boxes, policies, notifications, contracts . . .), rather than promoting effective good data protection practices."[209] These findings track earlier research about the impact of the Privacy Act—the law governing the treatment of personal information by government agencies and the fullest embodiment of FIPPS in the United States context—by privacy law pioneer Ron Plesser. Plesser found that "agencies by and large find the Privacy Act, in short, to be an annoyance. There is usually a person or two on the General Counsel's staff of most agencies whose job it is to see that the agency or Government department complies with the technical requirements of the Act of in other words, stays out of trouble."[210] He reported that the one individual responsible for the Privacy Act in the Department of Health and Human Services spent, "most of his time guiding his 'clients' through the maze of the Privacy Act so that they can obtain their goals rather than as a voice for privacy in that massive agency, which deals with millions of privacy-related files every day."[211] In sum, he found the tendencies towards bureaucratization that rules can promote.

---

[207] *Id.* at 88

[208] *See supra* text at nn. __-__.

[209] Rand Europe, *Review of the European Data Protection Directive* 39 (2009) (commissioned by UK Information Commissioner's Office).

[210] David Flaherty, Protecting Privacy in Surveillance Societies quoting from *Who cares about privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress*, House Committee on Government Operations (Subcommittee on Government Information, Justice, and Agriculture) (Washington D.C., 1983) p. 237-238.

[211] David Flaherty, Protecting Privacy in Surveillance Societies quoting from *Who cares about privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress*, House Committee on Government Operations (Subcommittee on Government Information, Justice, and Agriculture) (Washington D.C., 1983) p. 237-238.

By comparison, the account of privacy on the ground has reveals a set of interactions that have amplified the "voice[s] for privacy" external to, and inside of, regulated corporations. Indeed, this account adds to an increasing number of studies that reveal the importance of purposive agency and "collective action" in shaping discourse in an organizational field to facilitate the construction of meaningful substantive regulatory norms.[212]

Central the construction of such norms were the activities of the Federal Trade Commission. The FTC's activity diverges from command-and-control governance, but also contrasts sharply with the "reticent regulator" approach that studies have found permits the subversion of public norms in organizational fields.[213] Specifically, its behavior adopts many of the methods that scholarship on "New Governance" models of regulation suggest will best leverage the strengths of legal ambiguity.[214] Such approaches emphasize dynamism and collaboration. They emphasize the regulator's ability to draws recurrently from "experience at the relatively local level" and changing challenges as they arise, in order "continually to update the standards all must meet,"[215] and its capacity to "harness the power of new technologies, market innovation, and civic engagement to enable different stakeholders to contribute to the project of governance."[216] As such, new governance is "both top-down and bottom-up."[217]

The Commission's emphasis on making privacy management practices and failures transparent, bolstered by the disclosures forced by state security breach legislation, surfaced metrics for assessing corporate activity over time,[218] and benchmarks

---

[212] Hayagreeva Rao, et al., *Power Plays: How Social Movements and Collective Action Create New Organizational Forms*, 22 RES. IN ORG. BEH. 239, 242 (2000) (studying "the construction of new organizational forms as a political project involving collective action").

[213] Bamberger, *Technologies of Compliance*, *supra* note __ at 35 (discussing failures in oversight of implementation of broad risk-management mandates).

[214] *See See* Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342, 342–50 (2004) (describing the recent shift from the traditional "New Deal" regulatory era to a "Renew Deal" governance paradigm in which government, industry, and society "share responsibility for achieving policy goals").

[215] Michael C. Dorf, *The Domain of Reflexive Law*, 103 COLUM. L. REV. 384, 384 (2003) (reviewing JEAN L. COHEN, REGULATING INTIMACY: A NEW LEGAL PARADIGM (2002)).

[216] *Id*. at 264.

[217] Dorf, *supra* note __, at 384.

[218] *See* Michael C. Dorf & Charles F. Sabel, *A Constitution of Democratic Experimentalism*, 98 COLUM. L. REV. 267, 314–23 (1998) (discussing how agencies can take advantage of their vantage point on the behavior of multiple firms to develop "rolling best practices" by collecting data from regulated entities about what works and what does not, and then disseminating that information back, through education and capacity building); *see also* Bradley C. Karkkainen et al., *After Backyard Environmentalism: Toward a Performance-Based Regime of Environmental Regulation*, 44 AM. BEHAV. SCIENTIST 692, 692–709 (2000) (providing, in the environmental context, a model in which administrative agencies develop the architecture for gathering and analyzing information across local contexts as a part of the regulatory and education process).

for improvement[219]—the type of measures that both permit external accountability, and spur changes in organizational management. By publicizing the debates over privacy policy, such transparency further coupled privacy performance with dynamic pressure from evolving market perceptions, and especially to consumer protection.

Moreover both the availability of detailed information, and the wide range of participatory procedures the FTC provided has empowered privacy advocacy, and enabled the tremendous rise of a movement of advocates central to developing "frames that justify, dignify, and animate collective action,"[220] around "privacy"—a "concept that leaves a lot to be desired" as "a clear organizational principle to frame political struggle."[221] Indeed, as one advocate explained, "[i]n the United States it's the agency debates that are really important."[222]

This contrasts with the EU context, in that U.S. advocates are, a recent study documented, "far more likely to use the provisions within their relatively fragmented patchwork of laws, than (have) their European counterparts"[223] to advance privacy protection. In comparison, "[t]he privacy advocacy community has generally not made extensive use of the complaints investigation and resolution process under data protection law." Indeed, the study explains, "[i]t is indeed striking how few complaints have been lodged by European advocacy groups under their stronger and more comprehensive data protection laws" despite the fact that doing so "cost no money and very little time."[224] This paradox is attributed to the fact that European Data Protection Agencies are relatively "under-resourced," legally "constrained," and that some " do not have enforcement powers." Accordingly, advocates recognize that DPAs often "have to adopt a more pragmatic approach."[225]

The role of such advocates in shaping the discourse of an increasingly professionalized corps of corporate privacy officers—marked by some level of fluidity between the members of the two groups—has moreover introduced an element of advocacy within regulated organizations themselves, and within the professional associations whose members participate in the diffusion of privacy management practices across corporate boundaries.

The way in which these developments in publicity and participation can act as a "social license" constraining corporate activity "[r]esonate[s] with theories that

---

[219] *See* Sturm, *supra* note __, at 492–519 (discussing the importance of benchmarks in fostering meaningful organizational change and improvement).

[220] Colin J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE 1 (2008) (quoting Sydney Tarrow, Power in Movement: Social Movements and Contentious Politics 21 (1998))

[221] *Id.* at 2.

[222] *Id.* at 100 (quoting Chris Hoofnagle, formerly of the Electronic Privacy Information Center).

[223] *Id.* at 122.

[224] *Id.*

[225] *Id.* at 118.

emphasize the importance of a firm's social standing and in particular its economic stake in maintaining its reputation for . . . good citizenship."[226] In particular, they have aggregated otherwise dispersed market, consumer, and advocacy pressures to reproduce the types of forces that scholars of corporate regulation flag as important in producing "compliance-plus" behavior: visibility, community concern and threat to economic investment. In these contexts behavior can be "shaped by a far broader range of stakeholders within the 'organizational field' than regulators alone."[227]

Finally, at the core of this legal environment sits the FTC's entrepreneurial use of its enforcement power. To be sure, the ambiguous legal standards grounding the Commission's most powerful exercise of its regulatory power makes enforcement unpredictable, and incomplete. Yet in contrast to the "weak enforcement authority" described by Edelman in the employment context, the ambiguity of the FTC's legal directive provides its strength, and serves as a means to leverage the capacity of its entire regulatory approach.

The response to the FTC's roving enforcement authority described by every one of the privacy officers we interviewed—the way in which it spurred them to "look around corners" to consider the way in which an ambiguous consumer protection mandate could be applied to new practices, technologies and contexts—reflects dominant research on meaningful accountability in decisionmaking. Specifically, that research indicates that when decisionmakers face review by entities whose monitoring criteria are both well-specified and well-known, they behave as "cognitive miser[s]," "avoid[ing] mental calculations that require sustained attention, effort or computing power."[228] Yet that same research identifies other contexts in which the threat of review can force decisions to be more dynamic, thorough and thoughtful—when decisionmakers do not know the socially "acceptable" response—or more precisely, when those decisionmakers need to explain themselves to others.[229]

If, by socio-legal insights, regulated parties will adapt to a static set of external rules with a minimum of change, which, in turn, results only in cosmetic trappings of compliance, a dynamic model of regulation complicates the certainty of the threat, empowers those managers within organizations tasked with minimizing the threat in the competition for corporate resources, and creates a continuous external stimulus that must be translated into meaningful internal practice.[230] "Rather than perceiving the government demand as a single cost, the corporation's process of self-understanding may lead it" instead "to develop a relationship based on genuine compliance."[231]

---

[226] NEIL GUNNINGHAM, *ET AL.*, SHADES OF GREEN: BUSINESS, REGULATION, AND ENVIRONMENT 147 (2003)

[227] *Id.*

[228] Philip E. Tetlock, *Accountability: The Neglected Social Context of Judgment and Choice*, *in* 7 RES. IN ORG. BEH. 297, 311 (Barry M. Staw & L.L. Cummings eds., 1985).

[229] *Id.* at 314–21 (reviewing research evidence).

[230] Rubin, *supra* note __, at 387.

[231] Id.

CONCLUSIONS: PRIVACY UNDER THE MICROSCOPE

The privacy and data protection community is entering a two year period of reflection and introspection. 2010 marks the thirtieth anniversary of the Organization for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, the first international statement of fair information practice principles, and the OECD will kick off a review of the guidelines to identify areas for revision in early March.[232] A recent report reviewing the EU Data Protection Directive commissioned by UK Information Commissioner has proposed an alternative regulatory model oriented around outcomes.[233] And momentum has built for reconsidering the U.S. privacy framework. Both Congress and the Federal Trade Commission have signaled a commitment to deep reexamination of the current regulatory structure, and a desire for new models. Representative Rick Boucher (D-VA), chairman of the Communications, Technology and the Internet subcommittee of the House Energy and Commerce Committee, and Rep. Bobby Rush (D-Ill.), chairman of the House Energy and Commerce subcommittee on consumer protection, are reportedly in the final stages of drafting a bill to address internet and other technology-related privacy issues.[234] FTC Chairman Jon Liebowitz, and the Director of the agency's Bureau of Consumer Protection, David Vladeck, have both indicated a strong inclination to revisit the dominant privacy paradigm of notice and consent.[235] Vladeck has opined that, "[t]he frameworks that we've been using historically for privacy are no longer sufficient"[236] yet signaled uncertainty about how to move forward in protecting privacy's "dignitary"[237] interests in the commercial marketplace.[238]

---

[232] This groundwork will build a record for the review of the Guidelines in 2011 called for in the OECD's SEOUL DECLARATION FOR THE FUTURE OF THE INTERNET ECONOMY (2008). The aim is to determine whether the Guidelines should be revised or updated to address the current privacy environment, *see* SEOUL DECLARATION, at 10. The review process will begin in early March with an OECD Roundtable on the impact of the Privacy Guidelines, followed by a conference on privacy, technology and global data flows in October coinciding with the 32nd International Conference of Data Protection and Privacy Commissioners, and conclude on December 1, 2010 with a focus on the economic dimensions of privacy. http://www.oecd.org/document/35/0,3343,en_2649_34255_44488739_1_1_1_1,00.html

[233] *See* Robinson, *et al.*, *supra* note__, at xi-xii.

[234] Tony Romm, *House Lawmakers Preparing Key Cell-Phone Location Privacy Legislation*, THE HILL Feb. 24, 2010.

[235] Stephanie Clifford, *F.T.C.: Has Internet Gone Beyond Privacy Policies?*, N.Y. TIMES, January 11, 2010.

[236] Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, N.Y. TIMES, August 5, 2009

[237] *Id.*

[238] *An Interview With David Vladeck of the F.T.C.*, N.Y. TIMES Media Decoder, August 5, 2009 (discussing difficulty of identifying harm in context of behavioral advertising and how to frame dignitary interests).

Our account of privacy on the ground provides several important insights[239] for what we consider to be the "third wave" of privacy initiatives—tort laws being the first, data protection the second, and security breach notification and consumer protection analysis marking the beginning of the third.

First, our account supports the argument that calls for federal regulation structured exclusively around fair information practice principles are ill-advised. Our interviews indicated ways that FIPPS was insufficient to guide corporate behavior—particularly in times of profound technical or market change—and could create stumbling blocks for CPOs by positioning them once again as the "no" person. Thus many of our interviewees discussed efforts to transform internal perceptions about privacy from a compliance oriented, rule dominated, legal hurdle to be addressed at the end stage of product design, to a consultation and dialogue about how technical designs, business strategies, and policies can respect consumers' expectations and support trust in their companies. Our interviewees further suggested that, without a substantive touchstone, a data-protection regime can focus resources on developing a host of often meaningless consent processes,[240] which must be designed and redesigned in an effort to do better—where the meaning of "better" is unclear. They further predicted that the limitations of consent as the dominant fall-back for protecting consumer privacy would be exacerbated by the increasing trend toward networks, embedded devices, and increasingly personalized services.

While FIPPS remain an important touchstone for information privacy in the U.S., they should not be the exclusive touchstone for regulatory reforms. FTC enforcement aimed at protecting consumers' reliance on conventional information flows have brought greater substance and meaning to an area routinely critiqued for its formalism. In adopting a contextual analysis of privacy issues, the FTC's approach is responsive to the criticism of scholars and advocates who find that data protection can lead to a reductive construction of privacy and therefore resist working "within any fixed and guiding definition of what privacy means."[241] Viewing privacy as context-dependent protects against corporate and bureaucratic desires to reduce it to a set of *a priori* process-oriented rules, and the legalization and regularization that critics and proponents alike claim plague data protection. And protecting existing social norms about information use, rather than leaving each individual to the mercy of the marketplace, is key to addressing both collective and individual interests, for while

---

[239] There are certainly other core issues, such as those involving the preemption of state law, to which this paper does not specifically speak, and regarding which debate persists, *compare* Paul M.Schwartz, *Preemption and Privacy*, 118 YALE L.J. (2009) *with* Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868 (2009). For the time being we note that the debate over preemption largely brackets discussion of the issue of technical and scientific expertise issues, an "on the ground" issue which remains to be engaged.

[240] *See generally* Fred H. Cate, *The Failure Of Fair Information Practice Principles*, in CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' (2008) (discussing the failure of the notice and consent model to protect privacy meaningfully).

[241] BENNETT, THE PRIVACY ADVOCATES, *supra* note __ at 18.

"[p]rivacy self-defense operates at the individual level . . . surveillance operates at the collective level;" thus "the logics of surveillance require a considered, collective response."[242]

Second, our account identifies the important role that FTC plays in providing a forum for structuring and advancing a collective understanding of privacy among advocates, industry, academics and regulators. While the FTC's function as roving enforcement agency has been especially significant, its threat of coercive authority leverages an even deeper role in developing a cross-field understanding of privacy through workshops, fact-finding investigations, and other soft-law techniques to flesh out the meaning of its ambiguous privacy mandate. The collective engagement prompted through these regulatory choices has yielded both substantively groundbreaking outcomes—a divergence from *caveat emptor* with respect to privacy disclosures—as well as unique changes in corporate privacy management. The FTC's combination of enforcement threats with its centrality in fostering a social network of entrepreneurial privacy advocates offers a model for avoiding both the shortcomings of static top-down command-and-control regulatory approaches and the ways in which reliance on bottom-up self-regulation alone can subvert public goals by private interests.

This model should guide the choice and design of whatever regulatory institutions take the lead on information privacy in the corporate sector moving forward. They must both possess and use regulatory tools that exploit market, corporate and advocacy capacity to develop collective understanding of risks and solutions to future privacy problems.

Third, our account begins to illuminate the ways in which corporate privacy professionals impart meaning and structure to societal privacy concerns within corporations.

Debates about the establishment of a dedicated privacy agency in the United States emphasize the importance of governmental privacy expertise in shaping the rules governing corporate behavior.[243] Veteran privacy expert Robert Gellman contends that regardless of whether the U.S. chooses a highly regulated path forward or continues with on its current path, an expert federal privacy board would help achieve privacy objectives "more quickly, more efficiently, and consistently."[244] David Flaherty in his comparative study of the implementation of data protection and privacy laws in five countries, concluded that data protection must be entrusted to a "cadre of specialists" in a data protection authority [245] and attributed what he believed was the United States' poor privacy performance in large part to "the lack of an oversight agency."[246] Yet while

---

[242] Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*. 75 U. CHI L. REV. 1 (2008).

[243] For a thorough discussion of debates and various proposals to establish federal data privacy protection agencies see, Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L. J. 1183, 1192-97 (2003).

[244] Gellman, supra *note* __, at 1218.

[245] DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 389 (1992).

[246] *Id*. at 305

numerous proposals for a U.S. privacy agency have been proffered—some giving it regulatory authority, some merely advisory—none have garnered public or political support.[247] Indeed, recent legislative proposals to address privacy in the corporate sector seem to have abandoned the notion.

Yet if the vision of privacy expertise centralized within a free-standing government agency seems unlikely to be realized, a broad, vibrant and entrepreneurial "cadre of specialists" has developed in the private sector—within companies, advocacy organizations and academia. In the absence of a DPA staffed with data protection experts, and faced with increasing ambiguity as to what privacy requires, corporations depend on these new professionals to guide them through the challenges wrought by evolutions in technology and business practice. These professionals do not view themselves as compliance officers, but as norm entrepreneurs. Empowered by external threats that support their entrepreneurial efforts, they offer a unique capacity to embed privacy—as trust and consumer expectations—into the corporate psyche as well as business operations.

Choices about regulatory form will affect the ability to leverage these professionals—to empower them within their own organizations in ways that pushes privacy further into corporate culture. A decision to redirect privacy regulation towards more rule-bound governance, for example, might diminish the need for corporations to rely on high-level internal advocates of privacy concerns. As society becomes more pervasively networked, and privacy protection requires ongoing and on-the-ground attention to dynamic privacy interests that manifest in very different ways within different firms, then, institutional reforms should be attentive to preserving the benefits flowing from this embedded class of professionals, and seek to empower rather than displace them.

Finally, as the privacy community reflects upon the key global instruments of data protection, our account underscores the importance of empirical inquiry and thick institutional engagement in considering contested issues of regulatory strategy, technological complexity, social and institutional networks, and the protection of individual and communal interests in the private sphere. If privacy is to be protected in an increasingly connected world, debates over its formal regulation must increasingly be informed by the ways that today's frameworks operate on the ground.

---

[247] *See* Gellman, supra *note* __, at 1197.