ARTICLES

PRIVACY ON THE BOOKS AND ON THE GROUND

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

U.S. privacy law is under attack. Scholars and advocates criticize it as weak, incomplete, and confusing, and argue that it fails to empower individuals to control the use of their personal information. These critiques present a largely accurate description of the law "on the books." But the debate has strangely ignored privacy "on the ground"—since 1994, no one has conducted a sustained inquiry into how corporations actually manage privacy, and what motivates them.

This Article presents findings from the first study of corporate privacy management in fifteen years, involving qualitative interviews with chief privacy officers identified by their peers as industry leaders. Spurred by these findings, we

* 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, Michael Birnhack, Beckwith Burr, Danielle Citron, Mary Culnan, Lauren Edelman, Alex Fowler, Bob Gellman, Mark Gergen, Roseanne Greenspan, Chris Hoofnagle, Bob Kagan, Colin Koopman, Mark Lemley, Toby Levin, Maryanne McCormick, David Medine, Helen Nissenbaum, Anne Joseph O'Connell, Richard Purcell, Joel Reidenberg, Ira Rubinstein, Pamela Samuelson, Jason Schultz, Ari Schwartz, Paul Schwartz, Dan Solove, Jeff Sovern, Peter Swire, Eric Talley, Jennifer Urban, John Yoo, and other participants in workshops at the UC Berkeley Center for the Study of Law and Society, the 2009 Privacy Law Scholars Conference hosted by the George Washington Law School and the UC Berkeley School of Law, the 2009 Workshop on Federal Privacy Legislation at the NYU School of Law Information Law Institute, the Jerusalem Forum on Regulation and Governance at Hebrew University, the Tel Aviv University School of Law, the University of San Diego Law School, the 2009-2010 annual CIPLIT Symposium on Intellectual Property at the DePaul University College of Law, and the 2009 Women's Institute in Summer Enrichment sponsored by TRUST; for excellent research assistance by Marta Porwit Czajkowska, April Elliot, Kim Fox, Ilan Goldbard, Alisha Montoro, Parichart Munsgool, Sarah Ruby, Quinn Shean, Tatyana Shmygol, Sara Terheggen, James Wang, and Andy Wiener; and for excellent administrative assistance from Rebecca Henshaw and Jean S. Hayes.

present a descriptive account of privacy "on the ground" that upends the terms of the prevailing policy debate. This 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 emphasis on substance: preventing violations of consumers' expectations of privacy.

This "grounded" account should inform privacy reforms. While widespread efforts to expand consent mechanisms to empower individuals to control their personal information may offer some promise, those efforts should not proceed in a way that eclipses robust substantive definitions of privacy and the processes and protections they are beginning to produce, or that constrains the regulatory flexibility that permits their evolution. This would destroy important tools for limiting corporate overreaching, curbing consumer manipulation, and protecting shared expectations about the personal sphere on the Internet and in the marketplace.

INTRODUCTION

Scholars and advocates charge that U.S. law fails to protect privacy adequately. The dominant critique denounces the existing patchwork of privacy statutes as weak, incomplete, and fractured. It decries the absence of an agency dedicated to data protection and the consequent lack of clear guidance, oversight, and enforcement. And it argues that the U.S. privacy framework fails to provide across-the-board procedures that empower individuals to control the use and dissemination of their personal information.

Such critiques present a largely accurate description of the privacy law "on the books." But the debate has strangely ignored privacy "on the ground." Indeed, since 1994, no one has conducted a sustained inquiry into how corporations actually manage privacy and what motivates them.

That year, 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. Policies in important areas were nonexistent, 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 midlevel managers who lacked substantive expertise, played "particularly sub-

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

2. *See id.* at 4, 135-36 (documenting "a persistent policy/practice gap").

servient 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 midlevel manager: "The top executives rarely ask for [privacy] policy implications of . . . new uses of information. If anybody worries about that, it's my [midlevel] 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. This tendency was exacerbated because privacy was viewed as a goal in tension with core operational aims—an organizational phenomenon made worse 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 set of principles and a framework of more individualized industry codes, based on "Fair Information Practices" Principles (FIPPs). This approach emphasizes vindication of individual rights through mechanisms like notice and consent in decisions about the use of personal information and 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. While they differ in detail, reform proposals generally concur that increasing the corporate attention and resources devoted to privacy and improving substantive privacy outcomes requires a model of protection adopted throughout Europe: omnibus

3. *Id.* at 4.

4. *Id.* at 82.

5. *See id.* at 139. *See generally id.* at ch. 6 (describing "Ambiguity All Around").

6. *Id.* at 207 (emphasis omitted).

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

8. Specifically, Smith recommended a Data Protection Board with advisory powers to field complaints and to assist corporations in developing codes of acceptable practice. These codes would be drafted pursuant to a codified set of principles developed through consultation with industry. *See id.* at 217-24.

9. *See id.* at 209-24.

10. *See id.* at 210.

FIPPs-based privacy principles in law or binding codes, interpreted and monitored by the kind of independent privacy agency for which Smith called.

Yet in their constancy, these proposals to reform "privacy on the books" have largely failed to take account of a more recent sea change in corporate practices "on the ground"—and have thus ignored a curious paradox for normative assessment.

Between 1995 and 2010, corporate privacy management in the United States has undergone a profound transformation. 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 6500 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. PricewaterhouseCoopers and others conduct privacy audits across multiple sectors. 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 managing large and well-resourced staffs. Yet these changes cannot be attributed to the prescription born of the dominant critique. U.S. privacy regulations remain fragmented and ambiguous, having failed to shed their siloed and sectoral emphasis. U.S. privacy regulation has largely eschewed a commitment to robust FIPPs. Congress has declined to follow the European model of a dedicated privacy administrator.

This Article, presenting the initial findings of the first empirical research into corporate privacy practices in fifteen years, seeks to address this paradox. It draws on semistructured qualitative interviews with chief privacy officers (CPOs)[11] 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 Part II, although the leading CPOs we interviewed worked at heterogeneous firms, their responses evidenced considerable coherence on several points. First, they consistently reflected a profound shift in the definition of privacy and its treatment. Each of the corporate privacy leaders defined information privacy as more than "informational self-determination" protected by formal notice and consent, introducing a substantive notion of privacy rooted in *consumer expectations*. They understood the meaning of "privacy" to

11. Although all of those interviewed were the senior corporate officer responsible for privacy in their firms, most, but not all, had the title "chief privacy officer." To preserve anonymity, we use this title for all.

depend on the beliefs and assumptions of consumers as to the appropriate treatment of individual information and personal identity—expectations that 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 protects the "trust" of those whose information is 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 U.S. sectoral statutes and the EU Data Protection directive were credited in some instances for firms' initial commitment of resources and personnel, and for the establishment of a regulatory floor, the path these professionals would take was influenced by two other regulatory developments: the rise of the Federal Trade Commission's (FTC's) role as an "activist privacy regulator" advancing an evolving consumer-oriented understanding of privacy; and the passage of state security breach notification (SBN) laws as a means for binding corporate performance on privacy to reputation capital.

Finally, the interviews indicated a variety of nonlegal phenomena central to the formation and diffusion of the legal notion of privacy compliance as consumer harm prevention. These phenomena include the role of both technology changes and third-party advocates in making consumer privacy protection a market-reputation issue, and the importance of the professionalization of privacy officers as a force for transmitting consumer-expectation notions of privacy from diverse external stakeholders, and related "best practices," between firms.

The conclusions that can be drawn directly from this first phase of empirical inquiry are necessarily limited. Specifically, the views reflected in these interviews do not, in and of themselves, provide evidence of corporate attitudes towards privacy more generally. The sample is small, and it focuses only on the self-reporting of identified industry leaders. Additionally, this inquiry as yet does not seek to measure outcomes, but rather focuses on reports of subjective understandings and related practices.

At the same time, the feedback from these interviews can be instructive in several ways. First, it—along with other data regarding the management practices and decision processes surrounding privacy put into place in the nine firms studied[12]—suggests a set of elements common to firms with privacy managers identified as leaders. These elements, in turn, will provide the basis for a broad-based survey of privacy attitudes and practices among representa-

12. These elements are discussed in Kenneth A. Bamberger & Deirdre K. Mulligan, *Catalyzing Privacy: New Governance, Information Practices, and the Business Organization*, 33 LAW & POL'Y (forthcoming 2011).

tive firms, to determine the breadth and depth of convergence.

Second, the interviews direct scholarly attention to elements of regulatory practice, and to participants who shape the legal approach in the privacy field, that are often neglected in the dominant "on the books" narrative. Prompted by this direction, Part III of this Article looks to independent legal and historical sources to develop a new account of U.S. privacy "on the ground." It documents the uniquely American way in which the privacy field has augmented the largely individual rights-based and process-oriented privacy protections with a substantive concern for preventing violations of consumers' expectations about the treatment of information about them. Specifically, this account explores how the emergence of the FTC 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 interacted in reconstructing privacy norms in consumer terms, and participated in the diffusion and institutionalization of those norms.

Finally, as Part IV argues, the privacy leaders' responses in the interviews regarding the manner in which different ways of framing privacy might shape corporate approaches to its protection, in combination with the descriptive account of developments in the privacy field, indicate important directions for debates about both privacy law's substance and its form. As to substance, the leaders' responses offer texture to arguments regarding the incompleteness of a reliance on formal notice and consent mechanisms 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. The survey responses provide concrete examples of the ways in which a procedural understanding of privacy protection framed around informational self-determination may be insufficient in guiding corporate decisionmakers, ex ante, in making choices about the technologies they employ in products or processes. The responses also identify 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 a number of theorists have recently suggested will best vindicate individual and societal interests: those emphasizing subjective expectations over objective formalism, dynamism in the face of technological advance, and application by context in light of governing norms.

Moreover, the account of privacy on the ground offers indications for debates over regulatory form. While the dominant account argues for greater uniformity and specificity in privacy law, this account suggests the possibilities offered by governing privacy through flexible principles. It highlights the ways in which a regulator's entrepreneurial deployment of a broad and imprecise legal mandate, combined with SBN laws' reliance on information disclosure rather than behavioral mandates, centered a robust multiplayer discourse about privacy to focus market pressure and executive resources. While Smith saw

ambiguity as a "bug," it may now be an important "feature," central to the increase in corporate time and attention devoted to privacy.

This research, as this Article's Conclusion describes, suggests ways that the prevailing debate over the adequacy of U.S. information privacy law "on the books" might be diversified, just as Congress, the Obama Administration, and international organizations are revisiting national and global approaches to privacy. While bolstered procedural mechanisms for enhancing informational self-determination might be needed, pursuing that goal in a way that eclipses broader normatively grounded protections, or constrains the regulatory flexibility that permits their evolution, may destroy important tools for overcoming corporate overreaching, consumer manipulation, and the collective action problems raised by ceding privacy protection exclusively to the realm of individual choice.

I. REEVALUATING THE DOMINANT CRITIQUE OF 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 criticizes existing regulation for its market-based and sectoral approach to privacy protection in the corporate sector and contends 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 first articulated in the early 1970s. Legal academics and privacy experts have labeled the U.S. approach "FIP[Ps]-Lite,"[13] 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 data protection agencies are 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 the normative and predictive conclusions adopted by many scholars and advocates—that policymakers should act under the belief that U.S. firms

13. *See* PRIVACY RIGHTS CLEARINGHOUSE, PRIVACY TODAY: A REVIEW OF CURRENT ISSUES (2010), http://www.privacyrights.org/ar/Privacy-IssuesList.htm; *see also Federal Agency Protection of Privacy Act: Hearing on H.R. 4561 Before the Subcomm. on Commercial & Admin. Law of the H. Comm. on the Judiciary*, 107th Cong. 67-73 (2001) (statement of Edmund Mierzwinski, Consumer Program Director, National Association of State Public Interest Research Groups), *available at* http://judiciary.house.gov/Legacy/mierzwinski050102.htm (making a similar assessment).

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 United States has often ignored changes in both the substantive definition of privacy and the mechanisms for its protection that have emerged in the United States since Jeff Smith's study, and the ways in which those developments have shaped corporate practice.

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"[14] or "the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others."[15] This rights-based conception of information privacy is embodied in a set of "Fair Information Practices" Principles, which provide the backbone of data protection laws in Europe and many other countries.

The Organisation for Economic Cooperation and Development's (OECD's) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, finalized three decades ago, provides an influential statement of FIPPs.[16] It articulates eight principles to "harmonise national privacy legislation and, while upholding such human rights . . . at the same time prevent interruptions in international flows of data."[17] 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

14. The term "information self-determination" was set forth in a German court decision limiting the intrusiveness of the census. *See* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, ENTSCHEIDUNGEN DES BUNDESVERFASSUNGSGERICHTS [BVERFGE] 65, 1984, *translated in* 5 HUM. RTS. L.J. 94, 97 (1984).

15. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

16. ORG. FOR ECON. CO-OPERATION & DEV., *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, *in* OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 13 (2001) [hereinafter OECD PRIVACY GUIDELINES]; *see also* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 101-11 (1992) (describing the OECD principles).

17. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#preface (last visited Dec. 30, 2010).

collection—namely that "data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[18] They require data collectors to maintain information securely and emphasize the rights of data subjects to access and ensure the accuracy of personal information.[19] Thus while a FIPPs approach is rooted in a commitment to the substantive principle of individual self-determination, it relies largely on procedural protections, such as providing notice to the "data subject" and securing "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 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 [that] is not concerned with balancing data protection with other administrative and political values."[20]

These elements of privacy governance—comprehensive protections reflecting a commitment to self-determination 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 lacking on each dimension.[21] "[I]n contrast to the approach in many other nations," one scholar summarizes, "it is unusual in the United States to find any comprehensive privacy laws . . . that enumerate a complete set of rights and responsibilities for

18. OECD PRIVACY GUIDELINES, *supra* note 16, at 14.

19. Many FIPPs proponents consider such access rights to be "the most important privacy protection safeguard." BENNETT, *supra* note 16, at 103.

20. *Id.* at 239 (describing the arguments of DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, & THE UNITED STATES (1989)).

21. *See* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 358 ("Privacy protection in the United States has often been criticized . . . ."); Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes* 1 (NYU Sch. of Law Pub. Law & Legal Theory Research Paper Series, Working Paper No. 10-16, 2010), *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.").

those who process personal data."[22] Rather, regulation of the use and disclosure of personal information focuses on "specific, sectoral activities," such as credit reporting, health care, or electronic commerce.[23] Accordingly, informational privacy is governed by a variety of different laws, administered by different agencies—or sometimes by no agency at all[24]—setting forth divergent requirements governing the treatment of information by type and business sector.[25]

The resulting formal regulations provide uneven protection for personal information and unequal treatment, even for similarly situated industry players. Privacy protections, for example, often depend on the entity collecting personal information. Doctors and pharmacies are clearly covered by both federal and state privacy statutes protecting health information,[26] 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 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," which 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,[27] which regulates credit reporting activities, and the Privacy Act of 1974,[28] which regulates collection and use of data by government agencies, re-

22. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1632 (1999).

23. *Id.*

24. *See, e.g.*, Right to Financial Privacy Act (RFPA) of 1978, 12 U.S.C. §§ 3401-3422 (2006) (protecting the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records); Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. §§ 2510-2522 (extending restrictions against wiretaps to include transmissions of electronic data by computer); Video Privacy Protection Act (VPPA) of 1988, 18 U.S.C. §§ 2710-2712 (preventing disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual materials").

25. *See, e.g.*, Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), 15 U.S.C. §§ 6801-6809, 6821-6827 (empowering various agencies to promulgate data-security regulations for financial institutions); Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.) (regulating the use and disclosure of "Protected Health Information").

26. HIPAA's Privacy Rule, for example, regulates only the use and disclosure of certain information held by "covered entit[ies]," such as health care clearinghouses, employer-sponsored health plans, health insurers, and medical service providers that engage in certain transactions. 45 C.F.R. § 164.502 (2010).

27. Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681x).

28. Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a).

flect the FIPPs' "informational self-determination" rubric and include a full range of safeguards reflecting those principles' emphasis on notice, information, and consent.[29] 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 from perceived threats to other interests. Such concerns highlight privacy as a means of promoting social goals such as the efficacy of doctor-patient relationships 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."[30] Such instrumental approaches, and the balance between privacy and other values they implicate, were reflected in formative decisions regarding the governance of privacy on the Internet, which was characterized by limited government mandates supplemented by significant reliance on "self-regulation" by industry players.[31]

These elements of U.S. privacy regulation have left it ripe for critique. First, scholars, advocates, and politicians alike charge that the "patchwork"[32] nature of U.S. privacy statutes renders them underinclusive in their 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 that are unable to evolve as technologies and business practices change.[33] Thus, in many realms, privacy is protected only by market actors' self-regulation, which is bound to fail in the

29. *See* Solove & Hoofnagle, *supra* note 21, at 359-61 (discussing those two laws); *see also id.* at 357 (explaining how "emerging companies known as 'commercial data brokers' have frequently slipped through the cracks" of these laws).

30. Peter P. Swire, *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy*, 54 HASTINGS L.J. 847, 863 (2003).

31. *See, e.g.*, WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE 4 (1997) (promoting self-regulation as the preferred approach to protecting online privacy); Rubinstein, *supra* note 21, 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.").

32. *See* Priscilla M. Regan, *Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows*, 59 J. SOC. ISSUES 263, 275 (2003) (referencing "[t]he patchwork of sectoral regulation that has long confused the Europeans"); *CDT's Guide to Online Privacy*, CENTER FOR DEMOCRACY & TECH., http://www.cdt.org/privacy/guide (last visited Dec. 10, 2010) (discussing "the existing motley patchwork of privacy laws and practices"); Larry Dignan, *Senate, Web Ad Titans Joust over Behavioral Targeting*, BETWEEN THE LINES BLOG (July 9, 2008, 2:22 PM), http://blogs.zdnet.com/BTL/?p=9280 (quoting U.S. Senator Daniel K. Inouye as saying that he "fear[s] that our existing patchwork of sector-specific privacy laws provides American consumers with virtually no protection").

33. *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶ 48 ("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.").

absence of external incentives for information protection.[34]

Second, critics reject protections that do exist as "FIPPs-Lite,"[35] failing to embody the robust procedures embraced by Fair Information Principles.[36] They contend, moreover, that the turn to market-oriented rationales for privacy protection diminishes 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.[37]

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.[38] Thus, much of the dominant debate involves a normative claim that the current approach (in particular as contrasted with the EU data protection model)[39] fails 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 would define substantive privacy requirements for commer-

34. *See* CHRIS JAY HOOFNAGLE, ELEC. PRIVACY INFO. CTR., PRIVACY SELF REGULATION: A DECADE OF DISAPPOINTMENT 15 (2005), *available at* http://epic.org/reports/decadedisappoint.pdf ("Ten years of self-regulation has led to serious failures in this field."); Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771 (1999) (responding in part to CLINTON & GORE, *supra* note 31, critiquing U.S. reliance on self-regulation, and proposing FIPPs-based regulation).

35. *See* sources cited *supra* note 13.

36. Solove & Hoofnagle, *supra* note 21, at 358 ("Privacy experts have long suggested that information collection be consistent with Fair Information Practices.").

37. *See* Schwartz, *supra* note 22, at 1682 (arguing that market solutions to privacy devalue the potential for cyberspace to facilitate "democratic self-rule"); *see also* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 500-01 (1995) (discussing privacy's role in "reflect[ing] specific conceptions of governance" in the public and private sectors); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560 (1995) (tying the "individual self-determination" privacy affords to society's capacity for democratic self governance); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 734 (1987) ("[P]rivacy proves to be a prerequisite to the capacity to participate in social discourse. Where privacy is dismantled, both the chance for personal assessment of the political and societal process and the opportunity to develop and maintain a particular style of life fade.").

38. *See Consumer Privacy Legislative Forum Statement of Support in Principle for Comprehensive Consumer Privacy Legislation*, CENTER FOR DEMOCRACY & TECH. (June 20, 2006), http://www.cdt.org/privacy/20060620cplstatement.pdf (with signatories Eastman Kodak, eBay, Eli Lilly, Google, Hewitt, Hewlett-Packard, Intel, Microsoft, Oracle, Procter & Gamble, Sun Microsystems, and Symantec).

39. The EU model articulates, in an "omnibus" fashion, certain uniform restrictions on the processing of personal data intended to promote the Fair Information Principles set forth by the OECD: *notice* to the subject and *consent* to data's use; *limits* on data's use to the purpose stated; data *security*; *disclosure* of information collection; *access* to one's data; and methods for holding data collectors *accountable*. *See* OECD PRIVACY GUIDELINES, *supra* note 16. For a description of the EU Privacy Directive, see *infra* note 59.

cial firms based on FIPPs and authorize agency regulation as supplemented over time by court decisions interpreting their requirements."[40]

B. *Cracks in the Dominant Critique: 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 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 on and coordination of privacy issues 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 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.

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 composed of "non-existent policies in important areas and a persistent policy/practice gap."[41] 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.

40. Rubinstein, *supra* note 21, at 2.

41. SMITH, *supra* note 1, at 136-37.

1. *External indications of a sea change: the rise of the chief privacy officer*

The development of the corporate chief privacy officer (CPO) offers the most ready evidence of a sea change in privacy management.[42] In the late 1990s, companies in the financial and health sectors began creating CPO positions.[43] By 2000, companies in other sectors had created CPO positions as well[44]—often to great fanfare, as evidenced by numerous press releases announcing the appointments.[45] Companies' motivations for creating CPO posi-

42. One more anecdotal indicator of changes in corporate privacy management: in 1995, Smith referred to his study as the "study that almost wasn't." SMITH, *supra* note 1, at 51. 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. Many of the rejections followed an initial positive response and appeared to be driven by corporate lawyers and an overall sense that the topic of privacy was too sensitive and volatile to discuss publicly. *Id.* at 52, 54. Furthermore, while Smith eventually secured seven participants, even they remained 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 through the eyes of an outsider, but I imagine it will ultimately be painful." *Id.* at 54.

By contrast, the corporate officials we contacted for the study discussed below were willing, and some quite eager, to participate in our interviews. 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.

43. Christopher Brown, *Survey Finds Increasing Number of Firms Appointing Officers with Institutional Clout*, 1 PRIVACY & SECURITY L. REP. 78 (2002). It appears that the first U.S. privacy officer was Jennifer Barrett of Acxiom, an information services company. Barrett joined the company in 1974, working in many departments of Acxiom, and she became a vice president of the company in 1981. Since 1991, she has been responsible for managing privacy issues at Acxiom. *See* Press Release, Acxiom Global Privacy Leader Elected to Executive Committee at Center for Information Policy Leadership (Sept. 25, 2007), *available at* http://www.acxiom.com/news/press_releases/2007/pages/acxiomglobalprivacyleaderelectedtoexecutivecommitteeatcenterforinformationpolicyleadership.aspx; *Profile of Jennifer Barrett*, WALKER'S RES. (2009), http://www.walkersresearch.com/profilePages/Show_Executive_Title/Executiveprofile/J/Jennifer_T_Barrett_100003645.html.

44. For example, Ray Everett-Church (who claims to be the first CPO) was appointed to that position by AllAdvantage.com in 2000. *See* RAY EVERETT-CHURCH, http://www.everett.org/about.shtml (last updated Mar. 3, 2010).

45. *See, e.g.*, Yukika Awazu & Kevin C. Desouza, *The Knowledge Chiefs: CKOs, CLOs and CPOs*, 22 EUR. MGMT. J. 339, 340-41 (2004) (reporting the number of CPO positions newly created in various sectors from 1995 to 2003: 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)); Linda Rosencrance, *IBM Joins Chief Privacy Officer Trend*, COMPUTERWORLD, (Nov. 30, 2000), http://www.computerworld.com.au/article/74638/ibm_joins_chief_privacy_officer_trend (announcing IBM's appointment of Harriet Pearson to a newly created executive-level CPO position); Press Release, EarthLink Names Chief Privacy Officer (Dec. 13, 2000), http://www.earthlink.net/about/press/pressrelease.faces;jsessionid=E021D1B83DB8EA49FB568FFDEE997AFD?id=446 (announcing the appointment of Les Seagraves as CPO).

tions were mixed, ranging from assuring consumers that corporations who used personal information were not "a lot of evil-headed monsters"[46] to smoothing interactions with European regulators under the Safe Harbor Agreement.[47]

Quickly, the informational, training, and networking needs of these newly appointed CPOs were met by a new trade association, the Association of Corporate Privacy Officers. Formed in 2000, 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.[48] By 2003, IAPP claimed one thousand overall members.[49] In 2004, the association launched a certification program in corporate privacy compliance, which certified 350 professionals within a year.[50] And today, IAPP boasts more than seven thousand members from businesses, governments, and academic institutions across fifty-two countries,[51] runs a credentialing program in information privacy, the Certified Information Privacy Professional (CIPP), and runs a wide range of educational and professional conferences.[52]

Survey data, moreover, show that CPOs continue to become more common and more powerful within corporate structures. Within many Fortune 500 companies, CPOs are directors or C-level executives,[53] evidencing a perception of privacy as a strategic matter.

And corporate privacy resources expand outside firm structures as well.

46. John Schwartz, *Conference Seeks to Balance Web Security and Privacy*, N.Y. TIMES, Dec. 8, 2000, at C4 (quoting Richard Purcell, Microsoft's CPO).

47. Although the Safe Harbor Agreement does not require companies to appoint CPOs, the certification process requires the corporation to identify "a contact office for the handling of complaints, access requests, and any other issues arising under the safe harbor." *See FAQ 6—Self-Certification*, EXPORT.GOV, http://www.export.gov/safeharbor/eg_main_018253.asp (last visited Sept. 29, 2010).

48. *See Privacy Officers Association Changes Name*, 2 PRIVACY & SECURITY L. REP. 39 (2003); *About the IAPP*, PRIVACYASSOCIATION.ORG, https://www.privacyassociation.org/about_iapp (last visited Dec. 30, 2010).

49. *Privacy Officers Association Changes Name*, *supra* note 48.

50. Press Release, Int'l Ass'n Privacy Prof'ls, IAPP to Honor First Graduates of Landmark Privacy Certification (Oct. 20, 2005), https://www.privacyassociation.org/about_iapp/media/2005_10_20_iapp_to_honor_first_graduates_of_landmark_privacy_certification.

51. *About the IAPP*, IAPP, https://www.privacyassociation.org/about_iapp (last visited Dec. 30, 2010).

52. *Privacy Certification*, IAPP, https://www.privacyassociation.org/certification (last visited Dec. 30, 2010).

53. *See* Press Release, Int'l Ass'n of Privacy Prof'ls, 2005 Ponemon Institute, IAPP Announce Results of Annual Salary Survey (Mar. 11, 2005), *available at* https://www.privacyassociation.org/about_iapp/media/2005_03_11_ponemon_institute_iapp_announce_results_of_annual_salary_survey ("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.").

PricewaterhouseCoopers 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. Third-party privacy seal and certification programs have been adopted widely. 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.[54]

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."[55] The earliest evidence from this project—derived from semistructured 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 nonlawyers) 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.

This method of subject selection is not intended to elicit responses generalizable to firms broadly. The sample size is small and respondents are all identified field leaders. They all, moreover, work at large corporations (all but one are Fortune 1000 companies), the size that research suggests has a greater vested interest in establishing a positive reputation for compliance with regulators[56] and maintaining legitimacy with other external constituencies.[57] Our de-

54. For example, TRUSTe, an online privacy seal program, was founded in 1997 and currently has seals at 3440 web sites. *See TRUSTe Press Releases and Facts*, TRUSTE, http://www.truste.com/about_TRUSTe/press-room.html (last visited Apr. 10, 2010). The Better Business Bureau 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. *See Self-Regulatory Program for Children's Advertising*, CHILDREN'S ADVERTISING REV. UNIT, http://www.caru.org/guidelines/guidelines.pdf (last visited Apr. 10, 2010).

55. Other elements of this empirical project include broader surveys of U.S. firms, parallel interviews of European chief privacy officers, and comparative assessments of enforcement techniques.

56. *See* Alex Mehta & Keith Hawkins, *Integrated Pollution Control and Its Impact: Perspectives from Industry*, 10 J. ENVTL. L. 61, 64 (1998).

cision to interview identified leaders, then, seeks a window into something more specific: more granular insight into what elements and approaches are taken by those who others in the field identify as leaders, and the practices that provide legitimacy in the privacy domain. The representativeness of their answers, and the breadth of diffusion of their understandings of privacy and of the practices of the firms at which they work, will be tested through larger surveys.

The selection method, moreover, sought to uncover suggestions about developments in the privacy field more generally. Snowball samples tend to identify participants with thick social networks in a field; the interviews accordingly sought to capture the way in which "key informants" at the center of the privacy field reflect the broader privacy discourse of which they are a part. Similarly, because our respondents' corporations are likely to be more sensitive to shifts in regulatory structures and other external forces shaping the "social license" under which they operate, they may provide fruitful indicators of important changes in regulatory and market forces.[58] Thus our interviewees' reflection of the way the privacy discourse is framed is not presented in isolation, but in conjunction with a descriptive, historical, and documentary account of the development of the privacy field in which CPOs are only one set of players, as presented in Part III below.

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

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 within corporations; and (3) the role of external forces—specifically law, markets, advocates, and professions—in

57. *See* John Dowling & Jeffrey Pfeffer, *Organizational Legitimacy: Social Values and Organizational Behavior*, 18 PAC. SOC. REV. 122, 133-34 (1975).

58. Robert A. Kagan, *How Much Do National Styles of Law Matter?*, *in* REGULATORY ENCOUNTERS: MULTINATIONAL CORPORATIONS AND AMERICAN ADVERSARIAL LEGALISM 1, 19-22 (Robert A. Kagan & Lee Axelrad eds., 2000) (discussing pros and cons of case study approach to studying impact of regulations on corporate behavior).

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. sector-based regime. By their description, specific legal rules were important in establishing a floor and shaping certain "compliance-oriented" measures. At the same time, they played only a limited role in animating corporate processes and practices more broadly.

1. *The role of legal rules*

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 EU Privacy Directive.[59] They pointed, however, to the limited role that 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"

59. Directive 95/46/EC, 1995 O.J. (L 281) 31, provides an "omnibus" framework prohibiting the processing of personal data within the European Union in the absence of three conditions:

(1) Pursuant to a transparency requirement, unless the processing of personal data is deemed "necessary" for a variety of articulated reasons (performing or entering a contract; compliance with a legal obligation or performance of a task carried out in the public interest; to protect the data subject's "vital interests"; or for purposes of the legitimate interests of the party to whom the data are disclosed), it may occur only when the subject has given his or her consent. *Id.* at 40 (Article 7). Subjects also have the right to be informed when personal data are being processed, and to correct incorrect or incomplete data. *See id.* at 41-42 (Article 11).

(2) Personal data can only be processed for specified explicit and "legitimate purposes" and may not be processed further in a way incompatible with those purposes, *id.* at 40 (Article 6); and

(3) Data processing and storage (including length of storage) must be proportional to the purposes for which the data are collected. *See id.*

Pursuant to the Directive, personal data may only be transferred to parties in a third country if that country provides an "adequate" level of protection. *Id.* at 45 (Article 25). While the U.S. regime has not been determined to meet that standard, a "safe harbor" framework developed by the Department of Commerce in consultation with the European Union Commission permits individual U.S. firms to self-certify their privacy practices, thereby allowing transfers of personal information from European countries. *See* Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7, 8-9. A description of the Safe Harbor Principles can be found on the Department of Commerce's Website at http://www.export.gov/safeharbor/eu/index.asp.

shape particular privacy practices. In the words of others, they constitute the "starting point," "the backing" of an approach to privacy, or the "bottom" of the "privacy triangle." 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.

A respondent in the business-to-business sector explained that participation in the Department of Commerce-negotiated "Safe Harbor" program—which permits companies to self-certify their conformity with the requirements of the EU Privacy Directive[60]—plays a similar signaling function for business partners. Discussing their firm's choice between Safe Harbor participation and enforcing privacy safeguards through contracts with outsourcers, that CPO described that the decision in the direction of the Safe Harbor was "driven to a large extent by customers who started asking us, 'Are you members of the Safe Harbor?'" This customer push arose, then, because Safe Harbor certification worked as a "checkbox" indicating that a company met privacy adequacy standards and was much easier to manage than contract terms.

2. *The shortcomings of rules for privacy decisionmaking*

Yet at the same time, every respondent—whether in highly regulated industries or not—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. Issues of "security," "access," "notice," and "consent"—dominant in U.S.

60. *See supra* note 59.

FIPPs discourse—become questions of the reuse and repurposing of information, and the meaning of notice and consent when companies can manipulate huge amounts of data willingly supplied to them by consumers while still in formal compliance of the law.

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 toward "ubiquitous computing."[61] 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 reveal that a recipient falls into 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. 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 also an example of an environment that might reveal significant information about the activities of the inhabitant.[62] The computing and communication capacity in this setting resides in mundane everyday objects that lack the interfaces necessary to a notice and consent approach to privacy. Explained another way, previously unproblematic 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, 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

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

62. *See* Mikhail A. Lisovich, Deirdre K. Mulligan & Stephen B. Wicker, *Inferring Personal Information from Demand-Response Systems*, 8 IEEE SECURITY & PRIVACY 11, 11 (2010).

value coming back."

A number of respondents identified healthcare as one sector operating in this manner. Nontraditional medical providers—such as pharmaceutical companies and medical technology firms—play an increasing role in ongoing oversight and monitoring of health practices and outcomes. One 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. He explained that there are "different tumor types," "different types of diabetics," and 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 [the ethics] into consideration . . . 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, another CPO explained that these trends 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 trend toward ongoing remote communications with a product or service provider. Such technologies include, for example, 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, that CPO noted, this is an area in which FIPPs' 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? Proba-

bly not."

Finally, respondents spoke of 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 on the fact that they ensured that data transfers complied with the Safe Harbor or other regulatory requirements, or that they faced no legal obligation hindering their release of data to a government agency. Yet both instances clearly implicate deeper privacy questions about the potential compromise of personal information, questions for 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." Despite all 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 of privacy defined by consumer expectations. 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 strategic reasons respondents stressed the importance of developing "company law": consistent and coordinated firm-specific global privacy policies intended to ensure that a firm both complies with the requirements of all relevant jurisdictions and acts concordantly when dealing with additional business issues not governed by any particular regulation.

Respondents explained that, in drafting company-wide policies to ensure

global regulatory compliance, European law plays a large role in shaping the outcome.[63] "[W]e end up defaulting to the highest common denominator," explained one, "which really right now is Europe, and enforcing a fairly European looking code of conduct when it comes to privacy and information protection."

Critically, however, these policies extend beyond compliance with specific legal mandates to broader privacy policies focused on outcomes that, even if technically legal, implicate privacy concerns. Such beyond-compliance policies seeking to direct corporate practices are "consistent with our global corporate values, and consistent with evolving customer expectations."

2. *Privacy measured by "consumer expectations"*

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

Such "customer or . . . 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," and is "a core value associated with 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:

> [Y]ou 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

63. For a thorough examination of the global impact of the Data Protection Directive see Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMPUTER L. & SECURITY REP. 508, 517-18 (2008) (concluding that the "adequacy mechanism" in the Directive has proven an effective tool at spreading the EU framework globally, and discussing its specific impact on the United States through the adoption of the Safe Harbor Framework).

> 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: "[T]he 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."

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: the definitional ambiguity inherent in privacy regulation requires 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 expectations change 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 "external environment" shaping privacy, including "how the regulations or even the percep-

tion of the public changes." Accordingly, explained a fifth, corporate leaders must focus on "[w]hat'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, has 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, "[a]nd 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?" As a result, "I want to keep changing the way we're doing business so it is dynamic, so we are . . . trying to mitigate the risk of the day while keeping our core program in place. And so we're changing." Privacy, by this view, is "a journey, not a destination," a process by which "we . . . try to get everybody together to say, how do we mitigate risk?" and constant inquiry into "what's the next thing on the horizon?"

Accordingly, as we discuss in greater detail elsewhere,[64] our interviewees describe that they are incorporated into risk management structures at the highest management level, and privacy discussions have been moved out of compliance offices into the processes throughout the firm 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 [requests for proposals] in almost every selling instance. . . . And so these go on and on and that's something you never would have seen back in 2000.

Another described that "six, seven years ago, there was a change in the marketplace." Before then, "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." This lack of market pressure drove corporate practices accordingly: "[W]e're a product company [and] product companies produce what the market wants. [If t]he market doesn't want security, then you don't spend a lot of time thinking about security."

64. *See* Bamberger & Mulligan, *supra* note 12.

This new emphasis on consumers and markets, they described, arose in the context of several intertwined phenomena central to development of a new privacy definition: 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; societal and technological changes that strengthened the role of advocates and the media; and the professionalization of privacy officers themselves.

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,[65] since 1996 the FTC has actively used its broad 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 Commission'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 Commission'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

65. *See infra* Part III.

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" toward enforcement actions charging that firms had engaged in unfair practices, "[a]nd in the land of unfair[, standards are] pretty foggy." They explained that, under the unfairness standard, "there [are] always new situations that require an interpretation," in that "'unfair' is much more subjective, and the FTC has been pretty clear that they will figure out what it means at the time."

Others describe that the unpredictability of future enforcement by the FTC and parallel state consumer protection officials contribute to more forward-thinking and dynamic approaches to privacy policies, guided by a 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 firm and others, from one centered on compliance with ex ante rules to one animated by the avoidance of consumer harm. That respondent explained that, at the time of the privacy-compromising incident leading to the enforcement action, the firm had both security technology and privacy statements in place that were "fairly standard in corporate America" and "consistent with the best practices at the time."

Yet the Commission determined that these "best practices" failed to conform with what should be expected of firms holding themselves out as privacy-protective. As the CPO explained: "[W]hat 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.'" "Now, however," the CPO continued, it's "fairly fundamental," that companies must develop a "comprehensive program behind the website statement." But at the time,

> [W]e did our walk around with the FTC commissioners, I went with my general counsel, and it was a completely eye opening thing for [the GC] . . . . there were exchanges with the commissioners where . . . they basically said that . . . what we did was similar to . . . a nuclear warhead being dropped. . . . [T]he significance of that statement from a regulator who had the power to really hammer us hard . . . 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 firms. "You can't really go in and build I think solely from an appeal to the . . . greater good," one described, "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." By contrast, the threat of losing trust, and being subject to prosecu-

tion, created an important "fear aspect" or "risk aspect." Similarly, another described,

> I walked in [to firm officers and said:] '[L]ook 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 [the] 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," that CPO 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, yet another suggested, FTC enforcement actions under a "loose framework of Section 5" create an "extra layer [that] I don't think any privacy officer wants to skirt with." Accordingly, it changes the focus from the "strict compliance line" to "what can we do above and beyond 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 how the uncertain threat of FTC enforcement affected U.S. businesses:

> [I]t's kind of funny in Europe where they get all kooky about the Americans who want to dot every "i" and cross every "t." . . . [But] my enforcement agency . . . is the Federal Trade Commission [and] they enforce . . . 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,[66] 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.[67]

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 fo-

66. As of October 12, 2010, "[f]orty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information." *State Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATORS, http://www.ncsl.org/default.aspx?tabid=13489 (last updated Oct. 12, 2010).

67. *See, e.g.*, CAL. CIV. CODE §§ 56.06, 1785.11.2, 1798.29, 1798.82 (West 2010). 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.

cus," 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 potential downstream effect of corporate treatment of consumers' personal information. Specifically, as one CPO described, it "has heightened more people's understanding of the stakes inherent in managing data in a very real way," by shifting the analysis of risk from "the risk of losing data of IP or financial information," to the effects on the "poor individual." Previously, one might think "I just lost a credit card file[—]who gives a hoot? . . . [I]t's capped, so no big deal." Now, however, the response is "[H]oly 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."

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, . . . 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 . . . ."

The media pressure on this issue has accordingly given that CPO "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] the tip of the iceberg [of] what privacy challenges are, and the privacy program should be.'"

Further highlighting the distinct impact of the SBN laws, a respondent who heads privacy at a global company discussed their 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," that CPO said, because "[t]hey don't have security breach notification," which "changes behavior."

c. *Legal changes and the court of public opinion*

Our respondents explained that the high-profile activities of the FTC and the disclosures mandated by breach notification laws were particularly important because they dovetailed with already-occurring social and technological changes fueling privacy consciousness. This rise in consciousness both germi-

nated, 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, closed loop that is the media advocate," and stressed the importance of "what the CEO reads in the newspaper" to the "external environment." As one explained,

> right now, you see the P word all over the place. [I]t 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 what a third termed a "growing sensitivity by particularly senior executives to [privacy] things that are going on in the marketplace." This sensitivity, in turn, pushes companies 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."

2. *The role of professionalization in filling in ambiguous definitions of privacy*

In addition to emphasizing the development of an ambiguous and dynamic understanding of privacy through the interactions between regulators, advocates, and the role of the media in enhancing the corporate attention accorded privacy, the CPOs we interviewed point to the importance of the increasingly professionalized privacy-officer community in filling in the details of that dynamic, consumer-expectation oriented approach.

"Part of the privacy office challenge," described one CPO, "is what I call demystifying privacy." The CPO further explained,

> typically your boss and your boss's boss don't have a good, you know, preestablished 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, the interviewed privacy leaders described 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 in Part I, was made explicit. The association's publication and dissemination of information about 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 nontrivial component of their job duties involved collaboration with other members of the privacy sector; 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 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['s] 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 make better privacy decisions was in their interest. Helping "my competitor at XYZ Company do better," one described, is not "about competitive advantage." Rather, "[t]hat's about doing the right thing because if they screw up . . . 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 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 [or] a process for handling a security breach isn't going to give you a competitive advantage . . . 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

As described above, the marked increase in corporate attention and resources dedicated to privacy management since the publication of Jeff Smith's study over fifteen years ago could not have been spurred by the statutory developments Smith advocated—for in fact the United States held fast to its piecemeal approach to federal privacy legislation during this period, and eschewed the introduction of an omnibus privacy law and data protection agency. The interviews, by contrast, point to other atmospheric, institutional, and substantive developments—developments that play a minimal role in dominant critiques of the U.S. privacy framework—that track the changes in the logic and practice of corporate privacy management. 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 Part 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. The 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,[68] as the FTC emerged as a site of privacy norm interpretation and built upon this 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 Commission 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 Commission's entrepreneurial use of its enforcement powers, and by increased market pressures for privacy performance, these developments moved the privacy discourse from a focus on procedural mechanisms aimed at actualizing informational self-determination to an approach emphasizing the protection of substantive privacy norms, and shaped corporate privacy practice by creating a

68. *See* COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY 52-57 (2006) (discussing emergence of trust rhetoric in a range of global venues including the July 1997 EU conference on Global Information Networks and the 1998 OECD Conference in Ottawa).

"realistic threat of retribution for inattention."[69]

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 is "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 judgment call." Finally, privacy was tied to corporate reputation: "[T]he 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 United States 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 United States and in the European Union, arguments about the importance of privacy protection no longer sounded exclusively in the language of individual rights protection.[70] Instead, they also reflected a desire to facilitate electronic commerce and the free flow of information by building consumer trust. While tension between the European Union and the United States 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."[71]

By 1996, the rhetoric of consumer trust as a reason for business to attend to consumer privacy had become "something of a mantra" internationally.[72] That year, the OECD 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 use of the system so that it will be a commercial success."[73] In preparation for the EU

69. SMITH, *supra* note 1, at 214.

70. *See* BENNETT & RAAB, *supra* note 68, at 49-50.

71. CLINTON & GORE, *supra* note 31, at 16.

72. BENNETT & RAAB, *supra* note 68, at 52.

73. Org. for Econ. Co-Operation & Dev. [OECD], *Report of the Ad Hoc Meeting of*

Conference on Global Information Networks in Bonn in July of 1997, 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."[74] In the same year, OECD's report *Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet*[75] concluded that "consumer confidence is a key element in the development of electronic commerce," and that enforcement of privacy policies serves to bolster that confidence.[76] 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."[77]

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."[78] 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.-EU 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 United States and Europe. European countries were committed under the EU Data Protection Directive to a rights-based implementing framework with local Data Protection Authorities (DPAs) to monitor its application.[79] The DPAs, some of whose existence dated from the 1970s, were also organized around a rights-based framework.[80] Thus, in Europe the shift in privacy rhetoric occurred

Experts on Information Infrastructures: Issues Related to Security of Information Systems and Protection of Personal Data and Privacy, at 34, OECD Doc. OCDE/GD(96)74 (1996), *available at* http://www.oecd.org/dataoecd/32/50/2094252.pdf.

74. BENNETT & RAAB, *supra* note 68, at 53 (quoting Gunter Rexrodt & Martin Bangemann, Theme Paper (1997)).

75. OECD, *Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet*, OECD Doc. DSTI/ICCP/REG(97)6/FINAL (1998), *available at* http://www.oecd.org/dataoecd/33/43/2096272.pdf.

76. *Id.* at 4.

77. CLINTON & GORE, *supra* note 31, at 16-18 (describing privacy protection as essential, but noting privacy should not inhibit the free flow of information and arguing that self-regulation is the way).

78. BENNETT & RAAB, *supra* note 68, at 54.

79. Directive 95/46/EC, art. 28, 1995 O.J. (L 281) 31, 47; *see also supra* note 59.

80. *See* ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 74-75 (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").

against a well-developed framework and growing set of institutional players committed to conceptualizing information privacy through a lens of "data protection."[81]

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 United States 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 across the corporate sector generally 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 United States. 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"[82] and would retreat from shopping or banking online.[83] 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 "[s]uch use will only occur if consumers become confident and comfortable with the online world."[84] 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"[85] and claiming "there is a business advantage to be gained by companies that safeguard consumer in-

81. For a discussion of the process leading up to the directive and EU member states' laws, see Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 180-82, 191-95 (1999).

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

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

84. Letter from Frank C. Torres, III, Legislative Counsel, Consumers Union, to Donald S. Clark, Sec'y, Fed. Trade Comm'n (Mar. 26, 1999), *available at* http://www.ftc.gov/bcp/icpw/comments/conunion.htm (arguing for further privacy rules and standards on the grounds of increasing consumer trust).

85. GLOBAL BUS. DIALOGUE ON ELEC. COMMERCE, THE PARIS RECOMMENDATIONS 6 (1999), http://www.gbd-e.org/pubs/Paris_Recommendations_1999.pdf (presenting further evidence that the business community embraced at least the rhetoric of consumer trust).

terests."[86] When the FTC sought public comments in preparation for a consumer protection workshop in 1999, sixty-nine companies, nonprofits, and individuals responded—some in favor of self-regulation, and others arguing for new rules, but nearly unanimous in stressing the importance of consumer trust.[87]

The link between privacy, trust, and commerce was underscored by repeated consumer pushback after corporate privacy blunders. Companies announced information-sharing deals only to cancel them once masses of consumers made their objections known.[88] In July 1997, AOL scrapped a plan to sell subscribers' phone numbers to marketers.[89] 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 credit card.[90] In 1999, Intel reversed a plan to activate an identifying signature in its Pentium III chip when faced with advocacy filings to the FTC, pressure from industry partners, and a boycott.[91] 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 due to public pressure.[92]

While disputes over the optimal way to build trust waged on—consumer advocates favoring a regime of new privacy laws, the Clinton Administration and industry groups favoring industry self-regulation—all players increasingly framed their arguments in favor of privacy protection in instrumental terms: the

86. ALLIANCE FOR GLOBAL BUS., A GLOBAL ACTION PLAN FOR ELECTRONIC COMMERCE 22 (2d ed. 1999), http://www.oecd-ilibrary.org/science-and-technology/a-global-action-plan-for-electronic-commerce_236544834564.

87. *Public Comments Received*, FED. TRADE COMMISSION, http://www.ftc.gov/bcp/icpw/comments (last updated July 8, 1999) (listing all commentators and links to their comments, with nearly every comment making at least a passing mention of consumer trust before launching into the commentator's vision of privacy protection).

88. *See* Bruce Horovitz, *AmEx Kills Database Deal After Privacy Outrage*, USA TODAY, July 15, 1998, at 1B (listing other companies "that recently changed course after consumers balked").

89. *Id*.

90. *American Express Cancels Deal with Database Firm*, PLAIN DEALER (Cleveland), July 16, 1998, at 3C; Horovitz, *supra* note 88.

91. 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).

92. Mark Boal, *Click Back: Privacy Hounds Bring DoubleClick to Heel—For Now*, VILLAGE VOICE, Mar. 7, 2000, at 35 ("Months of backlash from privacy advocates forced DoubleClick to abandon its scheme. CEO Kevin O'Connor said his company was wrong to stake out territory not yet covered by government and industry standards. 'I made a mistake,' he said."); Fred Vogelstein, *Minding One's Business*, U.S. NEWS & WORLD REP., Mar. 13, 2000, at 45 (discussing decision to abandon plan to link offline and online data profiles "in the blink of an eye" because "Americans decided DoubleClick's business practices were not to be trusted").

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 FTC—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*

It is in this context that the FTC emerged,[93] 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.[94] "We recognized," explained former FTC Chairman Robert Pitofsky, speaking about his time at the Commission, "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."[95]

a. *Jurisdictional entrepreneurship*

This development was not predetermined by the terms of the Commission's statutory mandate to police "unfair or deceptive acts or practices."[96] As Jodie Bernstein, Director of the FTC's Bureau of Consumer Protection from 1995-2001, remarked, "[i]t didn't quite fit into 'deception or unfairness' for us to say, 'Everybody out there ought to be required to protect people's privacy.'"[97] But the substantive imprecision and procedural breadth inherent in the

93. The FTC had developed expertise on privacy as the agency responsible for rulemaking and enforcement under several sectoral statutes. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 776 (3d ed. 2009); RICHARD C. TURKINGTON & ANITA L. ALLEN, PRIVACY LAW: CASES AND MATERIALS, 428, 476, 478, 482, 496-97 (2d ed. 2002).

94. *See, e.g.*, Christine A. Varney, Comm'r, Fed. Trade Comm'n, Privacy in the Electronic Age, Address Before the Privacy & American Business Conference (Nov. 1, 1995) (transcript available at 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).

95. Interview by Brooksley Born with Robert Pitofsky, Former Chairman, Fed. Trade Comm'n, in Wash., D.C., 155 (Mar. 30, 2004) (transcript available at http://www.dcchs.org/RobertPitofsky/3_30_04.pdf).

96. 15 U.S.C. § 45(a) (2006).

97. Interview by Vicki Jackson with Joan Z. Bernstein, Dir. of Consumer Prot., Fed. Trade Comm'n, in Wash., D.C., 240 (May 1, 2000) (transcript available at http://www.dcchs

FTC Act left the Commission the space to play an increasingly important role in framing the debate. Beginning in 1995 with a public workshop to identify the Internet revolution's consumer protection and competition implications, and continuing with similar programs over the following several years, the FTC began to chart its own privacy agenda.[98]

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 that failed the test of "adequacy"—which included the United States[99]—U.S.-based multinationals, other firms with a global presence, and 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 self-certify privacy practices sufficient for trade with European partners.[100] These negotiations culminated with the European Commission approval of the "Safe Harbor Privacy Principles" (Safe Harbor Agreement) in July 2000.[101]

Throughout the extended and contentious process of negotiating the Safe Harbor Agreement, there was heavy pressure on U.S. industry to demonstrate capacity to self-regulate and for the United States to provide 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 FTC to fill this gap. A critical component of the Safe Harbor Agreement was the FTC's commitment to enforce privacy statements and to prioritize complaints by EU citizens.[102]

With the Safe Harbor's signal, the FTC was now relatively insulated

.org/JoanZBernstein/050100.pdf).

98. For an overview of the FTC's activities through 1996, see *Workshop on Consumer Privacy on the Global Information Infrastructure*, FED. TRADE COMMISSION, http://www.ftc.gov/bcp/privacy/wkshp96/privacy.shtm (last visited Oct. 16, 2010). For an overview of completed and planned work as of 1999, see Interview by Brooksley Born with Robert Pitofsky, *supra* note 95, at 155-65.

99. *See supra* note 59.

100. For an in-depth discussion of the connection between the EU Directive and privacy developments in the United States and other countries, see Birnhack, *supra* note 63.

101. Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7.

102. The European Commission's Decision 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.

Id.

against suggestions that its nascent privacy activities were beyond its inherent authority. The FTC 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 marketplace, and the FTC's 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. By contrast, it had substantial discretion to define what practices were unfair and deceptive,[103] and possessed wide latitude as to the institutional methods available for shaping the perceptions of legal requirements. In the privacy arena, it employed this authority to convene FTC Advisory Committees[104] and workshops,[105] request[106] and issue[107] reports, work with and place pressure on industry to develop self-regulatory codes of conduct and transparent privacy practices,[108] and safeguard personal information.[109] In all, the FTC leveraged its doctrinal latitude and institutional breadth to facilitate a

103. *See, e.g.*, FTC v. R.F. Keppel & Bro., 291 U.S. 304, 310 (1934) ("Neither the language nor the history of the Act suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories."); FTC v. Raladam Co., 283 U.S. 643, 648 (1931) ("'Unfair methods of competition' . . . 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.'" (citation omitted)).

104. *See, e.g.*, FED. TRADE COMM'N, FINAL REPORT OF THE FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY (2000), *available at* http://www.ftc.gov/acoas/papers/finalreport.htm.

105. The FTC 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 concerned credit reporting. *See Credit Reporting: Workshops*, FED. TRADE COMMISSION, http://www.ftc.gov/privacy/privacyinitiatives/credit_wkshp.html (last visited Aug. 28, 2010); *Financial Privacy: Financial Privacy Rule: Workshops*, FED. TRADE COMMISSION, http://www.ftc.gov/privacy/privacyinitiatives/financial_rule_wkshp.html (last visited Aug. 28, 2010); *Unfairness and Deception: Workshops*, FED. TRADE COMMISSION, http://www.ftc.gov/privacy/privacyinitiatives/promises_wkshp.html (last visited Aug. 28, 2010).

106. *See, e.g.*, AD-HOC WORKING GRP. ON UNSOLICITED COMMERCIAL EMAIL, REPORT TO THE FEDERAL TRADE COMMISSION (1998), *available at* http://old.cdt.org/spam.

107. Since 1996, the FTC has issued seventeen reports relating to privacy: seven staff reports and ten reports to Congress. *See Children's Privacy: Reports and Testimony*, FED. TRADE COMMISSION, http://www.ftc.gov/privacy/privacyinitiatives/childrens_reptest.html (last visited Aug. 28, 2010); *Financial Privacy: Pretexting: Reports and Testimony*, *supra* note 105; *Unfairness and Deception: Reports and Testimony*, *supra* note 105.

108. *See* FED. TRADE COMM'N, INDIVIDUAL REFERENCE SERVICES: A REPORT TO CONGRESS (1997); NETWORK ADVER. INITIATIVE, SELF-REGULATORY PRINCIPLES FOR ONLINE PREFERENCE MARKETING BY NETWORK ADVERTISERS (2000).

109. *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) (Jan. 7, 2001) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=507582 (discussing the initial five cases brought by the FTC under their "deceptive practices or acts" jurisdiction).

dialogue about corporate data practices, consumer understanding and expectations, and consumer harms.

b. *Developing a consumer expectations metric*

i. *Nonenforcement regulatory tools*

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.[110] These tools furthered three types of regulatory goals.

First, they greatly increased the transparency of corporate privacy practices. Through "sweeps" of both child-directed and general audience websites, the Commission documented and assessed information practices. Its fora encouraged stakeholders to do the same, fostering the production of additional surveys and research. This iterative documentation of corporate practices pressured industry to improve. The emphasis on best-practice improvement in turn bolstered trade associations and self-regulatory organizations that sought to stave off regulatory action. While the invisibility of corporate data practices had, as noted by Smith's 1994 study, made them largely immune to regulatory and public pressure, FTC initiatives brought corporate practices, and their import for consumers' expectations, into the light. This fueled a sustained debate about appropriate norms of behavior on an issue that was only previously addressed episodically, at best, by legislators in response to high-profile corporate privacy failures.

Second, the Commission employed its bully-pulpit power to motivate two important developments. Its calls for credible self-regulatory efforts were largely responsible[111] for the creation of two self-regulatory privacy seal programs[112] as well as a technical standard designed to reduce the transaction

110. *See generally* Kenneth A. Bamberger, *Normative Canons in the Review of Administrative Policymaking*, 118 YALE L.J. 64, 99 (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).

111. The need to demonstrate the "adequacy" of U.S. companies' privacy practices for purposes of the Safe Harbor guidelines, which permit individual U.S. firms to transfer personal information from European countries after a self-certification process, *see supra* note 59, also contributed to the creation of the seal programs. To be eligible to participate in the Safe Harbor guidelines, corporations must provide both recourse mechanisms to consumers and a process for verifying company adherence to privacy commitments. The seal programs provided one mechanism for meeting these obligations. *See generally Safe Harbor Workbook*, EXPORT.GOV, http://www.export.gov/safeharbor/eg_main_018238.asp (last updated Jan. 27, 2010).

112. *See BBB Online Business Program*, BBBONLINE, http://www.bbb.org/us/bbb-

costs associated with privacy decisionmaking through standardization and initially automated negotiation.[113] Furthermore, Commission persuasion was critical in encouraging companies operating online to post privacy policies. As discussed below, the publication of company policies making representations about 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.[114] The increased visibility into corporate practices facilitated evaluation by legislators, advocates, and the press.

Finally, the FTC's participatory fora 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,[115] participating in FTC advisory committees[116] and workshops, and engaging in agenda setting through the production of independent research[117] as well as interactions with FTC staff and commissioners. The Commission'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-1990s focusing much, if not all, of their energy on FTC engagement.[118] Workshops accorded an oppor-

online-business (last visited Apr. 10, 2010); TRUSTE, http://www.truste.com (last visited Apr. 10, 2010).

113. *See* Letter from Jerry Berman & Deirdre K. Mulligan, Internet Privacy Working Grp., to Fed. Trade Comm'n (Apr. 15, 1997), *available at* http://www.ftc.gov/bcp/privacy/wkshp97/comments2/ipwg049.htm (discussing the Platform for Privacy Preferences (P3P) Project and requesting participation in FTC Workshop on Consumer Information Privacy); *see also* LORRIE FAITH CRANOR, WEB PRIVACY WITH P3P 43-57 (2002) (discussing P3P's origin and relation to other external policy activities).

114. *See* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2046 (2000) (arguing that the FTC's promotion of privacy policies was a means for "the Agency to sink its jurisdictional hooks more firmly into the Internet privacy debate, and therefore the Internet").

115. *See, e.g.*, *Newsroom: Office of Public Affairs*, FED. TRADE COMMISSION, http://www.ftc.gov/opa/index.shtml (last visited Dec. 29, 2010) (offering press releases discussing four Commission enforcement actions—against CVS Caremark, Microsoft, Eli Lilly, and Lisa Frank—initiated after privacy advocates or the media brought the matter to the FTC's attention); *see also* COLIN J. BENNETT, THE PRIVACY ADVOCATES 124-25, 152, 155, 160-61 (2008) (discussing five other actions triggered by complaints from advocacy groups).

116. *See, e.g.*, FED. TRADE COMM'N, *supra* note 104 (discussing mechanisms to afford consumers access to personal information collected and maintained by commercial websites, mechanisms that are being designed by, among others, representatives from Consumers Union, the Electronic Privacy Information Center, the Center for Democracy and Technology, and the Electronic Frontier Foundation, as well as several privacy academics).

117. *See, e.g.*, AD-HOC WORKING GRP. ON UNSOLICITED COMMERCIAL EMAIL, *supra* note 106; CTR. FOR MEDIA EDUC., WEB OF DECEPTION: THREATS TO CHILDREN FROM ONLINE MARKETING (1996).

118. For example, Jason Catlett, president of Junkbusters, a for-profit company that

tunity for advocacy organizations to convey their views to a D.C. audience of reporters, Hill staff, trade associations, lobbyists, and industry executives. Through a compelling FTC complaint, moreover, an advocacy organization could leverage the resources, expertise, and investigative and enforcement capacity of a formidable agency.[119] These contexts provided a valuable stage for advocates to serve as a mouthpiece for concerns about privacy risks faced by the diffuse and broad-based population of consumers nationwide.[120]

These processes thus worked in two directions: Through them, the FTC built support for its work and gained an ongoing awareness of the ways in which consumer harms can arise from the breach of expectations wrought by the increased capacity and regularity of data collection. Simultaneously, advocates had a singular opportunity to shape an ongoing stakeholder dialogue in which the links between privacy, trust, and consumer expectation were nurtured—giving evolving content to the 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. The Commission's early cases focused on the accuracy of privacy notices, targeting business claims that were actively misleading under the Commission's jurisdiction to regulate "deceptive" practices.[121]

Progressively, however, the Commission broadened its enforcement focus to practices deemed "unfair"[122] and to transactions that were on the whole mis-

helped consumers reduce unwanted marketing communications, positioned himself as a privacy advocate for purposes of participating in FTC proceedings. *See* Letter from Jason Catlett, President, Junkbusters Corp., to Fed. Trade Comm'n (Oct. 18, 1999), *available at* http://www.ftc.gov/bcp/workshops/profiling/comments/catlett.htm; *see also* Amy Borrus, *The Privacy War of Richard Smith*, BUSINESSWEEK, Feb. 14, 2000, *available at* http://www.businessweek.com/2000/00_07/b3668067.htm (containing an FTC associate director's comments on the importance of independent privacy expert Richard Smith's work).

119. 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. *See* BENNETT, *supra* note 115, at 118-20.

120. *See generally* MANCUR OLSON, JR., THE LOGIC OF COLLECTIVE ACTION 44 (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 J. Stigler, *The Theory of Economic Regulation*, 2 BELL J. 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").

121. This approach, ironically, may have created a perverse disincentive for corporations to post privacy policies. *See* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 886 (2003) ("A company risks liability by making a disclosure, but does not risk accountability by remaining silent.").

122. *See, e.g.*, Complaint for Permanent Injunction and Other Equitable Relief ¶ 17,

leading despite legal disclosures. This change in regulatory approach unraveled settled understandings of the Commission'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 Commission 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 Commission'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. Spyware also challenged industry players 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.

Through a series of actions against companies that downloaded software without appropriate notice and consent procedures,[123] the Commission began to breathe substance into the process of consent. The majority of these cases involved "bundled software,"[124] where formal disclosures in end-user licensing agreements (EULAs) were found insufficient to provide notice of hidden soft-

Fed. Trade Comm'n v. ReverseAuction.com, Inc., No. 1:00CV0032 (D.D.C. Jan. 6, 2000), *available at* http://www.ftc.gov/os/2000/01/reversecmp.htm (alleging that violating a user agreement in order to send unsolicited and misleading commercial advertisements was likely to cause substantial, unavoidable harm to consumers, and thus constituted an unfair trade practice).

123. *See, e.g.*, Fed. Trade Comm'n v. Seismic Entm't Prods., Inc., No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788, at *2-3 (D.N.H. Oct. 21, 2004); Advertising.com, Inc., and John Ferber: Analysis of Proposed Consent Order to Aid Public Comment, 70 Fed. Reg. 46,175-77 (Aug. 9, 2005). Several of the FTC's spyware actions were informed by complaints filed by the Center for Democracy and Technology, which leads a group of anti-spyware software companies, academics, and public interest groups dedicated to defeating spyware called the Anti-Spyware Coalition (ASC). *Combating Spyware: H.R. 964, the Spy Act: Hearing Before the Subcomm. on Commerce, Trade, & Consumer Prot. of the H. Comm. on Energy & Commerce*, 110th Cong. 40, 42 (2007) (statement of Ari Schwartz, Deputy Director, Center for Democracy and Technology).

124. In "bundled" software offerings, the users understand that they are installing one program, but because they fail to read the EULA and the software attempts to hide itself in other 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. Advertising.com, Inc., 140 F.T.C. 220, 222 (2005) (declaring failure to adequately disclose bundled software that traced browsing "deceptive").

ware that eroded consumers' privacy in an unexpected manner, typically serving pop-up advertisements collecting information about consumer's online "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,[125] in addition to information narrowly considered "personally identifiable." This signaled that satisfying the formalities of contract law, which courts may accept as an affirmative defense,[126] would not preclude a deeper privacy inquiry or stricter requirements.[127]

FTC actions against companies for breaches 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.[128] While these and other security cases settled quickly, the resulting consent orders have established a de facto obligation to provide a "reasonable" level of security for personal information.[129] The reasonableness standard is fluid, evolving, and open to constant reinterpretation.

125. *Best Practices*, and other documents of the Anti-Spyware Coalition, similarly propose a richer contextual understanding of privacy issues based on "risk factors—those that increase the potential concern about a technology—and consent factors, basic notice, consent, and user control—that mitigate the risks." *See* ANTI-SPYWARE COALITION, BEST PRACTICES: GUIDELINES TO CONSIDER IN THE EVALUATION OF POTENTIALLY UNWANTED TECHNOLOGIES 1 (2007), *available at* http://www.antispywarecoalition.org/documents/documents/best_practices_final_working_report.pdf.

126. *See* Deirdre K. Mulligan & Aaron K. Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 22 BERKELEY TECH. L.J. 1157, 1205-11 (2007).

127. *See* Agreement Containing Consent Order at 4-8, Sony BMG Music Entm't, FTC No. 062-3019 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf (requiring that installation of software from a CD and the transfer of information by such software meets a heightened "clear and prominent" standard for notice and consent).

128. *See, e.g.*, BJ's Wholesale Club, Inc., 140 F.T.C. 465, 468 (2005); Complaint ¶ 9, CardSystems Solutions, Inc., No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf; Complaint ¶ 10, DSW Inc., No. C-4157, FTC File No. 052-3096 (Mar. 7, 2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf.

129. *See BJ's Wholesale Club*, 140 F.T.C. at 468-72 (2005) (alleging unfairness where no statements were made about security); Vision I Props., L.L.C., 139 F.T.C. 296, 299, 303-05 (2005) (alleging unfairness rather than deception); *see also* Michael D. Scott, The FTC, the Unfairness Doctrine and Data Security Breach Litigation: Has the Commission Gone Too Far? (Aug. 20, 2007) (unpublished manuscript), *available at* http://ssrn.com/abstract=1012232 (discussing and criticizing the FTC's data security cases under the unfairness doctrine); Andrew B. Serwin, The FTC's Increased Focus on Protecting Personal Information: An Overview of Enforcement and Guidance 2 (Nov. 22, 2008) (unpublished manuscript), *available at* http://ssrn.com/abstract=1305669 (discussing impact of FTC's corporate data security actions and promulgation of guidelines).

The ambiguity developed through FTC practice as to what privacy protection requires of corporations mirrors the sense of 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 Commission's move away from a limited notice and consent analysis has let loose a renewed conversation about privacy issues and what firms must do to treat consumers fairly and to 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 to 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,[130] these laws—of which forty-five 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 through disclosure."[131] Such tools require the disclosure of information about harms or risks as a means of "fortify[ing] either market mechanisms or political checks on private behavior."[132] In this case, disclosure requirements seek to prompt both; and while disclosures have provided important 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 brand implications. Privacy advocates have exploited media coverage of breaches to keep privacy and data protection on the front burner. Thus the Privacy Rights Clearinghouse maintains a chronology of data breaches,[133] while U.S. PIRG and Consumers Union have both leveraged the steady drumbeat of security breaches to build momentum for the

130. *See supra* notes 66-67 and accompanying text.

131. Cass R. Sunstein, *Informational Regulation and Informational Standing:* Akins *and Beyond*, 147 U. PA. L. REV. 613, 613 (1999) (describing the shift in informational regulation as "one of the most striking developments in the last generation of American law").

132. *Id.* at 614.

133. *Chronology of Data Breaches*, PRIVACY RTS. CLEARINGHOUSE, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last updated Aug. 31, 2010).

proliferation of model laws across states.[134]

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 prices,[135] and direct remediation and litigation costs[136] (recently calculated at $197 per record breached[137]), the bulk of the penalty to firms arises from lost business, a phenomena that has increased more than thirty percent between 2005 and 2007.[138] 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 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 reflects an increasing reality connecting between trust, brand image, and privacy prompted by the SBN laws.

Finally, the SBN laws created an incentive structure that drove companies to develop internal processes to manage risk.[139] The laws provided CPOs with a performance metric, both internally and with respect to peer institutions.[140] 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 organiza-

134. *U.S. PIRG's Model Legislation: The State Clean Credit and Identity Theft Protection Act*, U.S. PIRG, http://www.uspirg.org/financial-privacy-security/identity-theft-protection/model-law (last visited Sept. 2, 2010).

135. *See* Alessandro Acquisti et al., *Is There a Cost to Privacy Breaches? An Event Study*, *in* ICIS 2006 PROCEEDINGS 1563, 1573 (2006) (discussing the impact of a short-duration, 0.6% reduction in stock price on the day the breach is reported).

136. *See* Joris Evers, *Break-In Costs ChoicePoint Millions*, CNET NEWS (July 20, 2005, 6:35 PM), http://news.cnet.com/Break-in-costs-ChoicePoint-millions/2100-7350_3-5797213.html.

137. PONEMON INST., 2007 ANNUAL STUDY: U.S. COST OF A DATA BREACH 2 (2007).

138. *See id.*

139. *See* Deirdre K. Mulligan & Joseph Simitian, Assessing Security Breach Notification Laws (unpublished manuscript) (on file with authors) (identifying similar impact of SBN laws in areas such as asset management, portable media encryption, and the development of best practices).

140. *See* SAMUELSON LAW, TECH. & PUB. POLICY CLINIC, BERKELEY SCH. OF LAW, SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS 13-21 (2007), *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf (discussing internal impact of breach letters from the perspective of Chief Information Security Officers).

tions. 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*

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. But the combination of uncertainty regarding the FTC's evolution of privacy requirements and uncertainty regarding market responses spurred by data breach notifications was central to the striking trend towards corporate reliance on professional privacy management described in Subpart II.B.

Professionalism has long served as an important institution for mediating uncertainty in the face of environmental ambiguity.[141] In the privacy context, 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 relatively wide latitude to establish corporate practices and define their jobs.

141. *See, e.g.*, Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 AM. ECON. REV. 941, 947, 965 (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 Structures: Organizational Mediation of Civil Rights Law*, 97 AM. J. SOC. 1531, 1531 (1992) (discussing the importance of professional organizations in mediating legal ambiguity).

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 FTC—and the way in which its activities, together with the involvement of advocates, professionals, and market forces, helped frame a new discourse regarding privacy protection. Far from reducing uncertainty in the legal field, the Commission'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 mechanisms 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 when the Obama Administration and Congress consider 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.[142]

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 suggests the incompleteness of a reliance on formal notice and consent mechanisms 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. The account highlights technological and market changes that point to the frailty of an individual self-determination framework for guiding corporate responses to privacy issues raised by new products and services. And it indicates that a combination of field participants have refocused on a substantive approach of privacy protection that important theorists suggest best vindicates individual and societal interests: one that emphasizes objective expectations over subjective formalism, dynamism in the face of technological advance, and application by context.

Moreover, the account of privacy on the ground resonates with ongoing 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

142. *See* OECD PRIVACY GUIDELINES, *supra* note 16.

greater discretion in fulfilling legal goals.[143] Such regimes can produce merely symbolic or cosmetic self-regulation as participants in the legal field shape understandings of conformity that can undermine or contort the public goals they purport to advance. But the FTC's role in deploying its 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—suggests ways that administrative agencies can center the public voice in shaping both the law's framing and the "compliance-plus" mindset reflected by the interviewed privacy leaders. In this context, changes in the field may arise 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 of 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 the existing approaches emphasizing procedural tools to instantiate individual autonomy and personal choice.

This overlay does not deny the value of formal notice and consent protections or diminish the individual it is designed to protect or empower; rather, it eliminates the presumptions that the existence of procedural mechanisms are conclusive of an interaction's fairness and that the individual's subjective interests are the only ones that matter. 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, including the notice that accompanies it, falls outside some acceptable level of deviation from past consumer experience. Those inquiries rely on understandings of what consumers bring to a 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.[144] As a practical mat-

143. *See* Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377, 377-78 (2006).

144. Scholars have thus noted the need for approaches to privacy that "transcend that of individual benefit" yet do not deny the centrality of the individual in privacy's formulation. BENNETT & RAAB, *supra* note 68, at 44; *see also* PRISCILLA M. REGAN, LEGISLATING PRIVACY (1995) (documenting the comparative responsiveness of internal corporate debates on privacy to arguments about privacy as an enabler of some other collective social good, as

ter, new or unanticipated information flows will trigger legal scrutiny.

By diversifying legal understandings of privacy,[145] the development of the consumer expectations rubric provides an additional protection framework that pathbreaking work by scholars from diverse fields increasingly suggests can provide a more robust conception of privacy values deserving of defense. This framework offers a means to identify privacy problems ex ante in contexts that procedural protections cannot—a framework that is not reflected in FIPPs.

As these scholars explore, defining privacy as "informational self-determination" at once claims too much and protects too little. The notion that law should provide individuals with a common set of mechanisms for vindicating privacy requires that "[i]nformation 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 . . . be defined by individuals themselves."[146] As such, the substantive interest in the protection of privacy is collapsed 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 81 to 293 hours per year were they to skim the privacy policy at each website visited, and 181 to 304 hours if she actually read them.[147] In real terms, then, even the procedural right is often an empty one.

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."[148] 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.

---

opposed to as an individual right).

145. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 187 (2008) (discussing the "benefits of a pluralistic conception of privacy").

146. BENNETT & RAAB, *supra* note 68, at 9.

147. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 1, 17 (2008) (reporting ranges of the low point and high point estimates the study arrived at for skimming and reading policies). The study ultimately concludes that reading privacy policies costs approximately 201 hours a year at a value of $3534 annually per American Internet user, or about $781 billion annually for the nation. *Id.* at 19.

148. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE 148 (2010). This reflects 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." BENNETT, *supra* note 115, at 18.

This framing, moreover, often provides no "decision heuristic,"[149] 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.[150] 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.[151] Technology can both shape and be shaped by social context.[152] 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 "informational 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. When 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, our subjects described, they have sought, and found, normative guidance from the evolving metric of consumer expectations.

Recent work by philosopher and theorist Helen Nissenbaum explores the ways in which norms informed by social expectations can provide a far more robust and protective frame for privacy than its definition as a set of one-off individual choices. The latter, Nissenbaum describes, encourages the mistakes of "moral mathematics" described by philosopher Derek Parfit.[153] A focus on in-

149. NISSENBAUM, *supra* note 148, at 148.

150. *See generally* GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 135-36 (1970) (adopting Coasean insights regarding assigning liability to promote decisionmaking by the "cheapest cost avoider," and therefore the party best able to avoid harms).

151. *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 5-7 (2006) (describing the regulatory power of "code"); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 554-56 (1998) (discussing the regulatory power of technological capabilities and system design choices).

152. *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").

153. NISSENBAUM, *supra* note 148, at 241-42 (quoting DEREK PARFIT, REASONS AND

formational "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,"[154]—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."[155] 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.[156] 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."[157]

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 on the one hand, to entitlement and obligation to reuse or redisseminate on the other.[158] Thus, as Robert Post has described, privacy norms "rest[] not upon a perceived opposition between persons and social life, but rather upon their interdependence."[159]

These norms vary by context and evolve over time but at any one point embody the situational clues and understandings that inform individual cognition,[160] permitting efficient decisionmaking by precluding the need for individuals to engage in the impossible task of collecting and assessing all information

PERSONS 86 (1986)).

154. *Id.* at 242; *see also* Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. 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).

155. NISSENBAUM, *supra* note 148, at 129-30.

156. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 138 (2004).

157. *Id.*

158. *See id.* at 140-43.

159. Post, *supra* note 154, at 959.

160. *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, 480-82 (describing the normative perspective on decisionmaking, which emphasizes the selection of the applicable norm by first identifying the context as one in which the norm should prevail).

anew.[161] 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,"[162] and therefore their privacy.[163]

The privacy-protective power of substantive consumer expectations overlaid 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 Holdings Management Corporation,[164] for example, targets the company's use of an email invitation to join their "MY SHC Community" and download a program

161. "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: SOCIAL AND RATIONAL 198 (1957). "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, *supra* note 143, at 411. Thus, rather than "maximiz[ing]" their choices, humans consider only a few possible courses of action and "satisfice," HERBERT A. SIMON, ADMINISTRATIVE BEHAVIOR, at xxiv (2d ed. 1957), choosing to settle for a solution that is adequate.

162. *See* NISSENBAUM, *supra* note 148, at 158-59.

163. The consumer-expectations analysis we describe bears some conceptual similarity to the "reasonable expectation of privacy" test in Fourth Amendment law, *see* Katz v. United States, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring), a standard that has relentlessly eroded privacy as technologies of surveillance proliferate and networks collect and store data about individuals outside the home. Yet its use and impact are strikingly distinct. Rather than allowing the surveillance capacity of the technology to determine the privacy afforded, the FTC has centered existing norms as the arbiter of what privacy consumers ought to be afforded in light of technological change. The FTC's formulation is conservative in its bias, seeking to protect consumers from unanticipated information flows and the resulting loss of privacy.

Substantive and procedural distinctions provide one possible explanation for the disparate outcomes, despite the apparent similarity of the tests, and more importantly, suggest why the differences in outcome may persist. Although privacy in the Fourth Amendment context can be understood to vindicate a collective (social) interest, by maintaining the balance of power between individuals and the government, it is also frequently viewed as asocial, an interest asserted by individuals accused of criminal wrongdoing seeking to limit the ability of society to hold them accountable. Procedurally, then, Fourth Amendment privacy arises in the setting of an exclusion proceeding whereby evidence of wrongdoing has been found. By contrast, in the FTC context, privacy is framed as a societal interest asserted to maintain some balance of power between individuals and corporations in the marketplace. Procedurally, privacy claims arise in a context where individuals and society have done nothing to warrant intrusion into their lives. While privacy thus may continually yield to advances in technology that enhance law enforcement's ability to police individual behavior for the good of society, it may simultaneously rein in corporate behavior that seeks to upend traditional patterns of data collection and distribution that instantiate social norms. Balancing individual and corporate power may be framed as key to the fair functioning of the market place.

164. Sears Holdings Mgmt. Corp., No. C-4264, FTC File No. 0823099 (Aug. 31, 2009), *available at* http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf.

that ran in the background on users' computers. This program 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,"[165] 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.[166]

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[167]—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 writes: "I *do* have an expectation of privacy when it comes to my e-mail . . . even in [an] age of social-networking . . . most people still think of e-mail as a safe place for speaking privately with friends and family."[168] Thus, "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 "both shocking and unacceptable."[169] In turn, Kurt Opsahl of the Electronic Frontier Foundation describes the problem that Google "failed to provide users with the setting users had reasonably expected."[170] Thus, the appropriate privacy-protective behavior entails "mak[ing] secondary uses of information only

165. Complaint at 3, *Sears Holdings Mgmt. Corp.*, No. C-4264, FTC File No. 0823099, *available at* http://www.ftc.gov/os/caselist/0823099/090604searscomplaint.pdf.

166. *Sears Holdings Mgmt. Corp.*, No. C-4264, FTC File No. 0823099, at 3.

167. *See, e.g.*, Electronic Privacy Information Center Complaint, Request for Investigation, Injunction, and Other Relief Before the Federal Trade Commission ¶ 8 (Feb. 16, 2010), *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.").

168. Molly Wood, *Google Buzz: Privacy Nightmare*, CNET NEWS (Feb. 10, 2010, 5:48 PM), http://news.cnet.com/8301-31322_3-10451428-256.html.

169. *Id.*

170. Kurt Opsahl, *Google's "Buzz" Should Have Required Consent for Secondary Use of Private Information*, JURIST (Feb. 24, 2010, 9:35 AM), http://jurist.law.pitt.edu/hotline/2010/02/googles-buzz-should-have-required-user.php.

with clear, unequivocal user consent and control, and test[ing] these controls to ensure that the default settings match with the expectations of the user."[171]

In other instances, this turn to objective manifestations of privacy embodied in social norms has been used by the FTC to protect privacy where technological changes render traditional reliance on consent inoperative, or at least incomplete.[172]

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, FIPPs had offered no indication that a serial number on a chip would raise a privacy uproar. The Pentium serial number (PSN) was not tied to personally identifiable information, which was the trigger for FIPPs requirements as commonly understood at the time. Yet advocates singled out the PSN's capacity to track the actions of a computer across the Internet due to Intel's market penetration position in the Internet ecosystem and the ease with which even anonymized behavioral data can be used to detect individual identity.[173] The company had essentially embedded a tracking device in each computer—or in the colorful words of one advocate, "branded [it] with an identifier."[174] 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.[175]

B. *Implications for Debates over Regulatory Form*

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

171. *Id.*

172. 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," thereby removing data retention time frames from the private bargaining between individuals and corporations in the marketplace. FED. TRADE COMM'N, STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 47 (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

173. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1742-43 (2010) (discussing anonymization's failure to preclude reidentification techniques).

174. Declan McCullagh, *Intel Nixes Chip-Tracking ID*, WIRED, Apr. 27, 2000, *available at* http://www.wired.com/politics/law/news/2000/04/35950 (quoting David Sobel, General Counsel, Electronic Privacy Information Center).

175. *See Intel Pentium III Processor Serial Number*, CENTER FOR DEMOCRACY & TECH., http://oldandbusted.cdt.org/privacy/issues/pentium3 (last visited Aug. 28, 2010).

1. *Background 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 directs behaviors accordingly.

The shortcomings of command-and-control governance, however, are well recognized.[176] 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.[177] 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 "displacement of goals," by which compliance with partial but specific rules—originally promulgated as a means for achieving a regulatory goal—becomes the singular end.[178] 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 with little contextual knowledge, can disempower those within organizations who are charged with carrying out policies,[179] constraining internal pressures for greater resources and attention. It can alienate them from the goals behind the rules in

176. *See, e.g.*, Cass R. 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").

177. *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").

178. *See generally* ROBERT K. MERTON, SOCIAL THEORY AND SOCIAL STRUCTURE 199 (rev. & enlarged ed. 1957) (discussing the process of "*displacement of goals* whereby 'an instrumental value becomes a terminal value'").

179. *See* Alfred A. Marcus, *Implementing Externally Induced Innovations: A Comparison of Rule-Bound and Autonomous Approaches*, 31 ACAD. MGMT. J. 235, 250-51 (1988).

favor of a focus on formalism, which in turn leads to a routinization of decision processes[180] that may exacerbate human error when implementing external regulation.[181]

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.[182] 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.[183]

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, which create greater ambiguity regarding appropriate methods of compliance.[184] In contexts as diverse as securities regulation, employment discrimination, and domestic terror protection,[185] 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.[186]

This development has provided regulators with new tools for overcoming the challenges they face in identifying threats on the ground or private information about firm organization necessary for developing uniform top-down requirements for risk-mitigating behavior.[187] Framing legal mandates broadly

180. *See* Bamberger, *supra* note 143, 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").

181. *See* Marcus, *supra* note 179, at 235.

182. *See generally* Robert E. Scott & George G. Triantis, *Incomplete Contracts and the Theory of Contract Design*, 56 CASE W. RES. 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.").

183. *See generally* OLIVER E. WILLIAMSON, THE ECONOMIC INSTITUTIONS OF CAPITALISM: FIRMS, MARKETS, RELATIONAL CONTRACTING 32-34 (1985) (discussing "governance structure[s]" put into place to resolve future contractual uncertainty).

184. *See* Bamberger, *supra* note 143, at 390-92 (discussing the increased reliance on regulation that "articulates general goals," yet "make[s] few ex ante decisions about substantive detail"); 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").

185. *See* Kenneth A. Bamberger, *Global Terror, Private Infrastructure, and Domestic Governance*, *in* 2 THE IMPACT OF GLOBALIZATION ON THE UNITED STATES: LAW AND GOVERNANCE 203, 204 (Beverly Crawford ed., 2008); Ford, *supra* note 184, at 1; Sturm, *supra* note 177, at 462.

186. *See* Bamberger, *supra* note 143, at 386, 392 (discussing "[t]he [t]rend [t]owards [r]egulatory [d]elegation").

187. *See* Edward L. Rubin, *Images of Organizations and Consequences of Regulation*, 6 THEORETICAL INQUIRIES L. 347, 386 (2005) (describing the fact that regulators often impose

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.[188] 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.[189]

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 by incentives to expend effort in furthering public goals and by 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.[190]

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."[191] These critiques are deepened by the contributions of

counterproductive measures because they lack knowledge of particular firms' internal operations).

188. *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).

189. *See, e.g.*, Vincy Fon & Francesco Parisi, *On the Optimal Specificity of Legal Rules*, 3 J. INSTITUTIONAL ECON. 147, 147, 154 (2007) (presenting a model of optimal specificity of laws suggesting the use of standards instead of rules in areas undergoing rapid change).

190. *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 311, 312, 335 (Walter W. Powell & Paul J. DiMaggio eds., 1991) (discussing how external "[s]hocks" provided by legal institutions, macroeconomic conditions, or other organizations can provoke change in an otherwise stable field).

191. Kimberly D. Krawiec, *Cosmetic Compliance and the Failure of Negotiated Governance*, 81 WASH. U. L.Q. 487, 487 (2003); *see also* Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669, 714 (2010) (dis-

socio-legal scholars exploring the way that legal and organizational "field[s]"[192]—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"[193] compliance measures, procedures sufficient to signal "legal legitimacy while simultaneously limiting law's impact on managerial power" and preventing law from otherwise disrupting central firm structures.[194] Such practices, in turn, spread to other firms, which mimic what are perceived to be "successful" compliance models.[195] Especially in regimes typified by "weak enforcement mechanisms" and "inadequate and inconsistent feedback on what organizational practices are legal," then, regulated parties may use the "wide latitude to construct the meaning of compliance"[196] to adopt procedures that signal an organization's "legality," but avoid fundamental alteration to existing workplace culture.[197]

cussing the ways in which technological compliance systems "can permit individual actors motivated by organizational incentives and individual greed to manipulate their behavior in ways that mask its [risk]"); Lawrence A. Cunningham, *The Appeal and Limits of Internal Controls to Fight Fraud, Terrorism, Other Ills*, 29 J. CORP. L. 267, 271 (2004) (explaining that an emphasis on corporate internal control systems put into place to signal regulatory compliance with broad mandates "can lead controls to assume the character of ends in themselves, rather than means of achieving ultimate goals").

192. *See* Paul J. DiMaggio & Walter W. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, 48 AM. SOC. REV. 147, 148 (1983) (defining an organizational field as "those 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"); Lauren B. Edelman, *Overlapping Fields and Constructed Legalities: The Endogeneity of Law*, *in* PRIVATE EQUITY, CORPORATE GOVERNANCE AND THE DYNAMICS OF CAPITAL MARKET REGULATION 55, 58 (Justin O'Brien ed., 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").

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

194. Shauhin A. Talesh, *The Privatization of Public Legal Rights: How Manufacturers Construct the Meaning of Consumer Law*, 43 LAW & SOC'Y REV. 527, 533-34 (2009).

195. 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. *See* DiMaggio & Powell, *supra* note 192, at 150-52.

196. Edelman, *supra* note 141, at 1532, 1539.

197. By this process, scholars of employment law have shown, the "right to a nondiscriminatory workplace in effect becomes a 'right' to complaint resolution." Lauren B. Edelman et al., *Internal Dispute Resolution: The Transformation of Civil Rights in the Workplace*, 27 LAW & SOC'Y REV. 497, 529 (1993). Yet the right to complaint resolution "is far more superficial and entails fewer disruptions of routines than would a right to a nondiscriminatory workplace." 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); *see also* Talesh, *supra* note 194, at 527 (de-

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 payoff. "The ambiguous corporate privacy domain," he concluded, was a primary driver of the "poor policy-making dynamic—the drift-external threat-reaction cycle"[198] in which firms avoided proactive privacy management, and executives only confronted privacy issues in the face of specific, and limited, external threats. Ambiguity, moreover, was the condition "from which the other problems originate[d]."[199] 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 when such claims were in tension with other organizational goals, leading to an "emotional dissonance" that resulted in "redefining privacy"[200] 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.[201]

More recent inquiry, however, suggests flaws in privacy regimes that rely singularly on highly specified and proceduralized behavioral mandates. A recently released multidisciplinary report reviewing the European Union's Data Protection Directive, for example, finds that a focus on specific mandated process "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."[202] These findings track earlier research about the impact of the Privacy Act of 1974—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 who [sic] job is to see that the agency or Government department complies with the technical requirements of the Act or in other words, stays out of trouble.[203]

scribing 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").

198. SMITH, *supra* note 1, at 167.

199. *Id.*

200. *Id.* at 88.

201. *See* Rubinstein, *supra* note 21, at 2.

202. NEIL ROBINSON ET AL., RAND EUR., REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE 39 (2009).

203. *Oversight of the Privacy Act of 1974: Hearings Before the Subcomm. on Gov't In-*

He reported that the one individual responsible for the Privacy Act in the Department of Health and Human Services "spen[t] 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."[204] In sum, he found the tendencies towards bureaucratization that rules can promote.

By comparison, the account of privacy on the ground describes a set of interactions that has amplified such "voice[s] for privacy"—both external to, and inside of, regulated corporations. Indeed, this account adds to an increasing number of studies that reveal the potential of purposive "collective" participation in shaping discourse in an organizational field for constructing meaningful substantive regulatory norms.[205]

The activities of the FTC have been central to the construction of such norms. 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.[206]

Rather, the Commission's behavior offers a model in which regulatory ambiguity may provide a space within which regulators can play a more active role in catalyzing the field's development of legal meaning. Specifically, its course adopts many of the methods that scholarship on "new governance" models of regulation suggests will best leverage the strengths of legal ambiguity.[207] Such approaches emphasize dynamism and collaboration. They emphasize the regulator's ability to draw recurrently from "experience at the relatively local level" and changing challenges as they arise, in order to "continually . . . update the standards all must meet,"[208] and the regulator's capacity to "harness[] the power of new technologies, market innovation, and civic engagement to enable different stakeholders to contribute to the project of governance."[209]

fo., Justice & Agric. of the H. Comm. on Gov't Operations, 98th Cong. 237-38 (1983) (statement of Ronald L. Plesser).

204. *Id.* at 238.

205. *See, e.g.*, Hayagreeva Rao et al., *Power Plays: How Social Movements and Collective Action Create New Organizational Forms*, 22 RES. ORGANIZATIONAL BEHAV. 237, 238 (2000) (studying "the construction of new organizational forms as a political project involving collective action" (emphasis omitted)).

206. *See* Bamberger, *supra* note 191, at 703-04 (discussing failures in oversight of implementation of broad risk-management mandates).

207. *See, e.g.*, 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").

208. 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)).

209. Lobel, *supra* note 207, at 343-44.

As such, new governance is "both top-down and bottom-up."[210]

The Commission's emphasis on making privacy management practices and failures transparent, bolstered by the disclosures forced by state security breach legislation, brought to the surface metrics for assessing corporate activity over time[211] and benchmarks for improvement[212]—the type of measures that both permit external accountability and spur changes in organizational management. This trend was accelerated by the information disclosure mandated by state SBN laws. By publicizing the debates over privacy policy, such transparency further coupled privacy performance with dynamic pressure from evolving market perceptions and especially with consumer protection.

Moreover, both the availability of detailed information, and the wide range of participatory procedures the FTC provided, have empowered privacy advocacy and enabled the tremendous rise of a movement of advocates central to developing "frames that justify, dignify, and animate collective action"[213] around "privacy"—a "concept [that] leaves a lot to be desired" as "a clear organizational principle to frame political struggle."[214] Indeed, as one advocate explained: "In the United States it's the agency debates that are really important."[215] This contrasts with the EU context, in that U.S. advocates are, as a recent study documented, "far more likely to use the provisions within their relatively fragmented patchwork of laws, than . . . their European counterparts"[216] to advance privacy protection. Thus, "[t]he [European] privacy advocacy community has generally not made extensive use of the complaints investigation and resolution process under data protection law."[217] 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[s] no money and very little

210. Dorf, *supra* note 208, at 384.

211. *See* Michael C. Dorf & Charles F. Sabel, *A Constitution of Democratic Experimentalism*, 98 COLUM. L. REV. 267, 314-23, 403 (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, 692-94 (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).

212. *See* Sturm, *supra* note 177, at 492-519 (discussing the importance of benchmarks in fostering meaningful organizational change and improvement).

213. BENNETT, *supra* note 115, at 1-2 (quoting SYDNEY TARROW, POWER IN MOVEMENT: SOCIAL MOVEMENTS AND CONTENTIOUS POLITICS 21 (1998)).

214. *Id.* at 2.

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

216. *Id.* at 122.

217. *Id.* at 118.

time."[218] 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."[219] Accordingly, advocates recognize that DPAs often "have to adopt a more pragmatic approach."[220]

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—appears moreover to have 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 emphasize the importance of a firm's social standing and in particular its economic stake in maintaining its reputation for . . . good citizenship."[221] 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."[222]

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 render enforcement unpredictable and incomplete. Yet "ambiguous mandates and uneven enforcement may actually *heighten* law's cognitive salience, as organizations struggle to make sense of legal uncertainties and to develop shared definitions of acceptable compliance"[223]—a phenomenon described by our interviewees.

In each case the FTC's roving enforcement authority was identified as a spur to "look around corners," that is, to consider and predict the way in which an ambiguous consumer protection mandate might be applied to new practices, technologies, and contexts. In this sense, their accounts resonate with predictions from research on accountability in decisionmaking. Specifically, that research suggests that when decisionmakers face review by entities whose monitoring criteria are both well-specified and well-known, they behave as "cognitive misers," "avoid[ing] mental calculations that require sustained atten-

218. *Id.* at 122.

219. *Id.* at 118.

220. *Id.*

221. NEIL GUNNINGHAM ET AL., SHADES OF GREEN: BUSINESS, REGULATION, AND ENVIRONMENT 147 (2003).

222. *Id.*

223. Mark C. Suchman & Lauren B. Edelman, *Introduction* to THE LEGAL LIVES OF PRIVATE ORGANIZATIONS 1, 8 (Lauren B. Edelman & Mark C. Suchman eds., 2007).

tion, effort or computing power."[224] That same research, however, identifies other contexts in which the threat of review can force decisions to be more dynamic, thorough, and thoughtful: situations in which decisionmakers do not know the socially "acceptable" response or, more precisely, when those decisionmakers need to explain themselves to others.[225]

If, by these insights, regulated parties may adapt to a static set of external rules with cosmetic trappings of compliance that veil a minimum of internal change, a dynamic model of regulation that brings to bear both the uncertain enforcement threats and evolving social and market forces complicates the certainty of the threat and creates a continuous external stimulus that must be translated into meaningful internal practice.[226] "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."[227]

CONCLUSIONS: PRIVACY UNDER THE MICROSCOPE

The privacy and data protection community is entering a two-year period of reflection and introspection. The year 2010 marks the thirtieth anniversary of the OECD's *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, the first international statement of fair information practice principles, and the organization has begun a review of the guidelines to identify areas for revision.[228] A recent report reviewing the EU Data Protection Directive commissioned by the UK Information Commissioner has proposed an alternative regulatory model oriented around outcomes.[229] And momentum has built for reconsidering the U.S. privacy framework. Both Congress and the FTC have signaled a commitment to deep reexamination of the current regulatory structure, and a desire for new models. Representative Rick Boucher, chairman of the Communications, Technology, and the Internet Subcommittee of the House Energy and Commerce Committee, has introduced a bill to address In-

224. Philip E. Tetlock, *Accountability: The Neglected Social Context of Judgment and Choice*, 7 RES. ORGANIZATIONAL BEHAV. 297, 311 (1985).

225. *See id.* at 314-21 (reviewing research evidence).

226. *See* Rubin, *supra* note 187, at 387.

227. *Id.*

228. *See supra* note 16 and accompanying text. This groundwork will build a record for the review of the Guidelines in 2011, as the OECD called for in ORG. FOR ECON. CO-OPERATION & DEV., THE 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 id.* at 10. The review process began in early March 2010 with an OECD Roundtable on the impact of the Privacy Guidelines, followed by conferences on privacy, technology and global data flows and the economic dimensions of privacy. *See The 30th Anniversary of the OECD Privacy Guidelines*, OECD, http://www.oecd.org/sti/privacyanniversary (last visited Dec. 31, 2010).

229. *See* ROBINSON ET AL., *supra* note 202, at xi.

ternet and other technology-related privacy issues.[230] The FTC is revisiting the dominant privacy paradigm of notice and consent.[231] David Vladeck, director of the FTC's Bureau of Consumer Protection, has opined that "[t]he frameworks that we've been using historically for privacy are no longer sufficient,"[232] yet signaled uncertainty about how to move forward in protecting privacy's "dignity"[233] interests in the commercial marketplace.[234] Moreover, the Internet Policy Task Force, convened by the Commerce Department Office of the Secretary, with participation of the National Telecommunications and Information Administration, the National Institute of Standards and Technology, and the International Trade Administration, has begun a "comprehensive review of the nexus between privacy policy and innovation in the Internet economy."[235]

In this light, a grounded account of privacy suggests several cautions for reform.

The first involves the diversity of approaches to privacy governance. Bolstering and rationalizing procedural mechanisms for enhancing informational self-determination may provide desirable coherence and uniformity as contrasted with the current disjointed regulatory regime—especially as the European approach increasingly but inconsistently becomes part of the compliance mix through the Safe Harbor framework. Yet at the same time, pursuing that goal in a way that eclipses broader robust substantive protections, or constrains the regulatory flexibility that permits their evolution, may destroy important tools for overcoming corporate overreaching, consumer manipulation, and the collective action problems raised by ceding privacy protection exclusively to the realm of individual choice.

Our interviewees described a variety of contexts in which that approach failed to provide a norm to guide design decisions in a privacy-protective direction, echoing recent privacy work indicating that, without a substantive touchstone, data-protection regimes can focus resources on developing a host of of-

230. Tony Romm, *House Lawmakers Preparing Key Cell-Phone Location Privacy Legislation*, HILLICON VALLEY: THE HILL'S TECHNOLOGY BLOG (Feb. 24, 2010, 12:12 PM), http://thehill.com/blogs/hillicon-valley/technology/83395-house-lawmakers-preparing-cell-phone-location-privacy-bill.

231. *See* Stephanie Clifford, *F.T.C.: Has Internet Gone Beyond Privacy Policies?*, N.Y. TIMES MEDIA DECODER (Jan. 11, 2010, 4:03 PM), http://mediadecoder.blogs.nytimes.com/2010/01/11/ftc-has-internet-gone-beyond-privacy-policies.

232. Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, N.Y. TIMES, Aug. 5, 2009, at B1.

233. *Id.*

234. *See An Interview with David Vladeck of the F.T.C.*, N.Y. TIMES MEDIA DECODER (Aug. 5, 2009, 2:24 PM), http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc (discussing difficulty of identifying harm in the context of behavioral advertising and how to frame dignitary interests).

235. Notice of Inquiry on Information Privacy and Innovation in the Internet Economy, 75 Fed. Reg. 21,226, 21,226 (Apr. 23, 2010).

ten meaningless consent processes,[236] which must be designed and redesigned in an effort to do better—where the meaning of "better" is unclear. They further described ways in which the limitations of consent as the dominant fallback for protecting consumer privacy is exacerbated by the increasing trend toward networks, embedded devices, and increasingly personalized services. FTC enforcement aimed at protecting consumers' reliance on conventional information flows, by contrast, has brought greater substance to an area routinely critiqued for its formalism. 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 that critics and proponents alike claim plagues data protection. 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 "[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."[237]

Second, the experience of the FTC role in privacy governance should inform the choice and design of whatever regulatory institutions take the lead on information privacy in the corporate sector moving forward. Our account identifies the importance of the FTC forums in 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 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. The capacity for such balance arises directly from regulatory tools that exploit market, corporate, and advocacy capacity to develop collective understanding of risk, and solutions to future privacy problems.

Third, our account suggests the importance of attention to the role of corporate privacy professionals in translating privacy concerns within corporations. Debates about the establishment of a dedicated privacy agency in the

236. *See generally* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341 (Jane K. Winn ed., 2006) (discussing the failure of the notice and consent model to protect privacy meaningfully).

237. Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 201 (2008).

United States emphasize the importance of governmental privacy expertise in shaping the rules governing corporate behavior.[238] Veteran privacy expert Robert Gellman contends that regardless of whether the United States chooses a highly regulated path forward or continues on its current path, an expert federal privacy board would help achieve privacy objectives "more quickly, more efficiently, and more consistently."[239] 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[240] and attributed what he believed was the United States' poor privacy performance in large part to "the lack of an oversight agency."[241] Yet while 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.[242] 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, corporations, faced with increasing ambiguity as to what privacy requires, depend increasingly on a different "cadre of specialists"—those within companies, advocacy organizations, and academia—to guide them through the uncertainty wrought by evolutions in technology and business practice.

Choices about regulatory form will affect the ability to leverage these professionals' capacity to function as "norm entrepreneurs"—their ability to frame privacy concerns in ways that facilitate their integration into firm decisionmaking. 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 privacy experts, and in turn reduce their capacity to embed privacy into corporate culture and business operations. 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, institutional reforms should be attentive to marshalling external influences on the corporation in ways that enhance the potential benefits flowing from this embedded class of professionals.[243]

Finally, as the privacy community reflects upon the key global instruments

238. 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).

239. *Id.* at 1218.

240. DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 389 (1992).

241. *Id.* at 305.

242. *See* Gellman, *supra* note 238, at 1197.

243. *See generally* Bamberger & Mulligan, *supra* note 12, at 26-27 (discussing the "boundary-spanning" potential of high-level corporate privacy professionals).

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.