New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry

KENNETH A. BAMBERGER and DEIRDRE K. MULLIGAN

While the turn from traditional regulation to more collaborative, experimentalist, and flexible forms of governance has garnered significant academic focus, far less attention has been paid to the effects of such "new governance" approaches on regulated firms' understanding of the laws' demands, and on the structures employed within business organizations to meet them. This article targets this analytic gap by examining internal corporate practices regarding consumer privacy, an arena in which the Federal Trade Commission and the states have adopted new governance models. Using data from qualitative interviews with leading corporate Chief Privacy Officers, as well as internal corporate documentation, it examines the way privacy practices have been catalyzed in the shadow of new privacy governance approaches and the combination of regulatory, market, and stakeholder forces they seek to harness. Specifically, it suggests the convergence of a set of practices adopted by privacy officers identified as "leaders," regarding both high-level corporate privacy management and the integration of privacy into entity-wide risk management goals through technology, decision-making processes, and the empowerment of distributed expertise networks throughout the firm.

I. INTRODUCTION

Over the past decade, legal scholars have devoted considerable focus to the shift from traditional forms of static, rule-bound, top-down, "command-and-control" regulation, to new forms of governance that promote regulatory ambiguity, diversity, and revisability; that involve policy dynamism informed by experience and experimentation; that rely on transparency to create legal and market pressures for compliance; and that enlist stakeholders—including advocates, professionals, and regulated firms

Address correspondence to Kenneth A. Bamberger, Professor of Law, University of California, Berkeley—School of Law, Boalt Hall NA446 MC #7200, Berkeley, CA 94720-7200, USA. Telephone: (510) 643-6218; Fax: (510) 868-2013; E-mail: kbamberger@law.berkeley.edu; Deirdre K. Mulligan, Assistant Professor, School of Information, UC Berkeley, 102 South Hall, Berkeley, CA 94720-4600, USA. Telephone: (510)642-0499; Fax: (510) 642-5814; E-mail: dkm@ischool.berkeley.edu.

LAW & POLICY, Vol. 33, No. 4, October 2011 ISSN 0265-8240

themselves—in achieving policy solutions. Yet while the literature has offered increasingly robust explorations of "new governance" tools that regulators may employ in such collaborative and experimentalist endeavors, it has paid far less attention to the effects of these tools on regulated firms' understanding of the laws' demands and on the structures employed within business organizations to meet them. The legal academic spotlight, then, has largely taken a "top-down" vantage on the move away from top-down regulation; the bottom-up response remains largely unilluminated.

Our project targets this analytic gap. Specifically, we are interested in the ways in which firms have incorporated practices and structures intended to protect privacy in the treatment of personal information, an area in which existing statutory mandates have been supplemented in recent years by the ascendancy of the Federal Trade Commission (FTC) as an "activist" privacy regulator employing a wide variety of new governance techniques—a trend documented extensively in our earlier work (Bamberger and Mulligan 2011)—and by the passage by state legislatures of Data Breach Notification Laws, which require the publication to affected parties of breaches involving certain personal information.

The first step of the project, presented here, involves both qualitative interviews with nine Chief Privacy Officers (CPOs), identified as field leaders, and the collection of data as to internal privacy practices and management structures within their firms. It follows a landmark study of privacy practices in seven corporations conducted by management scholar H. Jeff Smith seventeen years ago (Smith 1994)—the most recent such examination—and evidences a marked shift in the field. At that time, the privacy arena was marked by systemic inattention and lack of resources. "[P]olicies in important areas" were "non-existent," and those that existed were not followed in practice (ibid., 4). Executive neglect signaled to employees that privacy was not a strategic corporate issue. Absent external pressure, corporate executives avoided action, a tendency exacerbated because privacy was viewed as in tension with the firm's core operational aims.

The contrast with the corporate practices we documented is striking. As the corporate privacy leaders we interviewed described, compliance with specific legal mandates—the driver of corporate action in 1994—plays only a limited role in their approaches to privacy. As we have discussed more fully elsewhere (Bamberger and Mulligan 2011), the firms' visions of what privacy requires has shifted from a focus on formal procedural protections—such as notice as to the use of personal information and an opportunity to consent to that use—to a more substantive understanding that privacy protection requires firms to take actions to avoid harms that are caused by the use of private information in ways that violate consumer expectations. This shift has occurred in the shadow of new and robust new governance methods adopted by the FTC and state regulators. It is these new governance initiatives that loom largest on the radar of the corporate privacy managers we interviewed. The dynamic nature of privacy under this definition, and the formidable

enforcement actions it informs, moved the CPOs, and the firms, to approach privacy as a risk to be managed rather than a matter of legal compliance.

Furthermore, as this article develops, our respondents described four trends in the architecture of internal corporate privacy management that they understood to be integral to this risk management function.

Two trends involve the rise of the Chief Privacy Officer function itself—nonexistent a decade ago—and the implications for the salience and form of privacy in corporate decision making. First is the increasing power of corporate privacy leaders within the corporate structure. Privacy officers we interviewed sat at their firms' senior management level—often within the "c"-suite. From this vantage, privacy was included in both top-down activities, such as employee training, as well as communications with the board of directors. CPO activities largely involved strategic, rather than purely operational, issues, and their participation in high-level fora for setting firm goals moved privacy from a subsidiary "add-on" to an issue integrated into strategic corporate decision making. In addition to their location in the corporate structure, moreover, our interviewees described the way the ambiguity of the external privacy environment fostered firms' reliance on their professional judgment and the concomitant autonomy and power such dependence affords them within their organizations.

Second is the external orientation of the high-level privacy officers we interviewed. Faced with uncertainty as to external demands on the firm resulting from the interplay between norms, technical and business changes, and flexible regulatory authority, they spend up to half of their time interacting with external stakeholders including regulators, advocates, and professional peers. Such deep and ongoing external engagement, they report, is essential for assessing the state of dynamic privacy norms, participating in their construction, and in turn translating them meaningfully into firm practices.

Our interviews, moreover, unearthed striking stylistic similarities in the operationalization of privacy along two additional dimensions. First, they describe the way that its framing as a risk management function has enabled the integration of privacy into core firm values. So understood, privacy is moved from a cost center to a functional concern on the level of product operability, manufacturing accuracy, and process effectiveness. This framing further allows privacy's inclusion into preexisting, and highly resourced, technological, management, and audit processes intended to manage risk, powerful systems that would not otherwise be developed to address privacy concerns alone.

Second, privacy is operationalized through a distributed network including both dedicated privacy professionals and specially trained employees within business units empowered with practices and tools that assist with identifying and addressing privacy during the design phase of business development. These distributed mechanisms, on the one hand, extend the reach of the CPO into the firm, creating a bidirectional system that communicates privacy objectives downstream while facilitating the identification of new

issues and escalation upwards. On the other hand, this architecture enhances the legitimacy and effectiveness of the privacy function by both engaging the business units in defining and tailoring privacy's operationalization within specific corporate environments and also placing responsibility for compliance with these agreed upon business-aligned privacy objectives with the senior executives within each unit.

The conclusions that can be drawn from these findings must be tentative. Our interviews explicitly focused on those firms and privacy officers identified as industry leaders, and the breadth of these practices awaits the broader survey of firms that constitutes our project's next phase. Moreover, organizational sociology suggests that the "institutionalization" of common behaviors across a field of practice may reflect those behaviors' cosmetic ability to signal legitimacy to outside observers, as distinct from their efficacy (DiMaggio and Powell 1983, 152).

Yet, at a minimum, our interviews report an emerging set of privacy-management practices among a subset of firms with identified privacy leaders, in the shadow of a new governance regime. And they suggest some indicia of success, as these architectures address failings identified by Smith (1994) over fifteen years ago and resonate with structures and practices that organizational scholars have proposed as most successful in prompting firm decision making to incorporate secondary mandates—here, the protection of privacy—alongside core operational aims.

II. THE CONTOURS OF NEW GOVERNANCE

A definition of new governance frequently begins by setting forth what it is not: conventional "command-and-control" measures by which regulators, in a top-down fashion, seek to achieve particular outcomes by articulating, specific, *ex ante*, universal rules requiring certain conduct or the achievement of particular measurable outcomes.

The shortcomings of such forms of regulation have been well documented. They prove less operative when regulatory goals are more complex (Sunstein 1991), as specific rules often cannot reflect the large number of variables involved in achieving multifaceted regulatory goals. The problem is compounded, moreover, when regulated entities are heterogeneous and contexts are varied, as one-size-fits-all rules cannot easily account for the ways in which risk manifests itself differently across firms (Lobel 2003; Sturm 2001). Regulators, furthermore, have neither the resources nor the vantage to attain the granular knowledge necessary to combat risk within individual companies (Bamberger 2006). And uniform, static, approaches to regulation are particularly inapt to contexts characterized by rapid changes in technology and market infrastructure.

At the same time, rule-based regulation systems can have detrimental effects on decisions within the organizations they govern, leading to a process

of bureaucratization that results in "goal displacement," by which compliance with partial but specific rules—originally promulgated as a means for achieving a regulatory goal—becomes the singular end (Merton 1957, 199). Moreover, an approach in which rules of action are communicated in a centralized top-down fashion and intended to be applied by others can disempower those within organizations who are charged with carrying out policies, constraining internal pressures for greater resources and attention (Marcus 1988). These effects can lead to routinized "check-the-box" forms of compliance and crowd out meaningful organizational attempts to achieve public policy goals (Bamberger 2006; March and Simon 1958).

To address these shortcomings in a variety of substantive contexts, scholars and policymakers have turned to a collection of regulatory approaches broadly termed "New Governance" (De Búrca and Scott 2006; Lobel 2004) While the category is a capacious one, two general themes are especially salient to the governance of privacy. On the one hand, the singular role of state experts in prescribing measures for achieving public goals is relaxed in favor of participation by a variety of stakeholders, as civil society, professionals, and market actors are engaged in the process of regulatory development, enforcement, and implementation (De Búrca and Scott 2006; Trubek 2002; Sturm 2001). On the other, fixed and static regulatory commands are eschewed in favor of legal mandates that permit for evolution and dynamism in the face of technological and normative developments and for variety in application by context (Lobel 2004).

These themes, accordingly, have significant implications for both the tools employed by regulators and their role in a system of governance. New governance approaches supplement, or sometimes replace, codified commands with more open-ended directives that leave significant discretion in their application—discretion that both permits evolving interpretation by administrative agencies themselves, and that leaves space for regulated firms to exercise their own judgment and expertise in experimenting with different methods of implementation (Bamberger 2006). They utilize limited enforcement resources strategically, to send signals and provide the "external shocks" (Fligstein 1991, 311) necessary to strengthen those within the organization responsible for taking the actions necessary to achieve policy goals (Black 2005; Ayres and Braithwaite 1992). They combine firm mandates with "soft" or nonbinding approaches such as dialogue with interested parties, speeches by regulators, and educational activities including workshops and the issuance of interpretive or guidance documents intended to shape corporate behavior outside the enforcement context (Rakoff 2000). They engage in activities to promote field transparency, such as the collection and publication of data and information-disclosure requirements (Karkkainen, Fung, and Sabel 2001; Sunstein 1999).

By the incorporation of such methods, the traditional administrative role of the state is altered. If, conventionally, regulators operated as a singular source of policy expertise and legal command, in a new governance model

they serve as the center of a regulatory and enforcement network. Accordingly, they develop processes that can draw on the expertise and input of a variety of parties in shaping and elaborating policy in ways that can overcome the informational obstacles to effective governance. They encourage and strengthen the hand of third parties, such as policy advocates, independent certification bodies, and professionals in and outside of regulated entities, who offer nonstate means of shaping norms of corporate behavior (Sabel and Simon 2004; Sturm 2001). As Michael Dorf and Charles Sabel (1998) explore in their influential model of new governance administration, moreover, government can serve as a locus for dynamic policy development, by encouraging experimentalism by regulated parties in the face of environmental change, and by using the results to develop benchmarks and "rolling best practices" that inform regulatory and enforcement strategies moving forward (314).

This suite of approaches, the literature on corporate compliance suggests, can have profound effects on the behavior of regulated firms. Collaboration with those firms and others with "on the ground" knowledge and expertise can lead to specific internal management choices reflective of granular challenges to the achievement of public goals (Coglianese 2001). Increasing the information available to market actors can harness the enforcement effects of market reputation, social movements, and private attorneys general, key elements to the "social license" under which firms operate and that spurs internal adaptation to external demands (Kagan, Gunningham, and Thornton 2003; Salancik, Pfeffer, and Kelly 1978). Market benchmarks and best practices can provide critical measures for directing internal decision making about firm resources (Sturm 2001). And uncertainty and dynamism in the meaning of legal requirements, combined with the shadow of legal enforcement, can strengthen those within regulated entities responsible for legal compliance (Edelman 1992). By this combination of coordination, education, and coercive functions, then, new governance approaches offer the capacity to create a continuous external stimulus on regulated parties, intended to force their approach to compliance away from static check-the-box processes, and catalyze the ongoing development of meaningful internal practices (Rubin 2005).

III. THE RISE OF THE NEW GOVERNANCE OF PRIVACY

The dominant account of U.S. privacy regulation focuses on "old" forms of governance—the multitude of requirements mandating particular corporate practices contained in statutes directed specifically at the corporate treatment of different subtypes of personal information. As is described in this section, we have elsewhere documented in substantive detail the way in which that account of privacy "on the books" ignores fundamental changes in the governance landscape "on the ground" (Bamberger and Mulligan 2011)—

specifically, it has largely overlooked the rise of new, and dominant, forms of privacy governance that reflect greater flexibility, collaboration, and the private behavior of regulated parties. This gap is not surprising, as it reflects the phenomenon by which a singular focus on legal texts "conceals rather than reveals or illuminates the presence and prevalence of new governance forms" (De Búrca and Scott 2006, 5–6). Yet a focus on these very forms is critical if one is interested in understanding corporate behavior, as they are ones our respondents report most important to compliance choices in the privacy arena.

A. PRIVACY-REGULATING STATUTES: REGULATION ON THE BOOKS

To be sure, formative decisions regarding the Unites States' governance of privacy in an age of Internet development chose the path of limited government mandates, supplemented by significant reliance on self-regulation by industry players (Clinton and Gore 1997). Fearful of stifling the growth of e-commerce in the face of rapid technological and market-structure development, both Congress and successive presidential administrations eschewed the enactment of "omnibus" privacy laws, comprehensive regimes that "codify a complete set of rights and responsibilities for those who process personal data" (Schwartz 1999, 1632). What statutory mandates do exist are limited by sector and type of information, prescribe limited, and largely procedural, protections against unauthorized use of information, and receive criticism as patchwork, piecemeal, underinclusive, and arbitrary (Center for Democracy & Technology 2010; Rotenberg 2001; Reidenberg 1999). European requirements affecting the behavior of U.S. firms trading internationally, moreover, focus on specific process-based, formalistic, and largely static, mandates obliging the provision of notice, and the receipt of consumer consent, before information is used. In the blunt assessment of one scholar, years of reliance on unsupervised self-regulation by corporate actors has led to "serious failures" (Hoofnagle 2005, 15). As the pace of technological and market change accelerated, both rule-based and purely self-regulatory approaches have become increasingly less relevant to the protection of privacy.

B. THE TURN TO NEW GOVERNANCE

As we have documented more fully elsewhere, however (Bamberger and Mulligan 2011), a separate set of developments in the privacy arena mark a sharp turn towards new governance. First, the FTC emerged, in the words of one of our respondents, as an "activist privacy regulator," pursuant to its statutory consumer-protection mandate to police "unfair or deceptive acts or practices" (15 USC § 45).[1] This trend has been strengthened by the enactment of state data breach notification statutes that revealed information about

how firms use and manage personal information, which has helped fuel a public conversation about data privacy and security.

The FTC's centrality to privacy governance involved some degree of jurisdictional entrepreneurship. For while the FTC was the agency responsible for rule making and enforcement under several specific sectoral statutes regulating privacy, including the Fair Credit Reporting Act, (15 USC § 1681 et seq.), which governs the accuracy, dissemination, and integrity of consumer credit reports, it only directed its general consumer-protection authority to information privacy in 1995, when it held its first of a number of public workshops to identify the consumer protection and competition implications of the globalization and technological innovation at the core of the internet revolution (Federal Trade Commission 1996, 1999). From that beginning, however, the FTC has become a laboratory of privacy norm elaboration (Hetcher 2000), seeking through its own and outside expertise, measurement, investigation, and sustained stakeholder engagement to define privacy's place in the new online marketplace, and its role as the leading consumer protection agency in shaping and enforcing practices to respect it.

The FTC has achieved this function by a combination of a number of new governance approaches, taking advantage both of its substantial discretion to define what practices falls under the broad and flexible "unfair and deceptive" standard, and wide latitude as to the institutional methods available for developing legal requirements.

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 numerous deliberative and participatory processes promoting dialogue with advocates, industry, and academia. The agency convened federal advisory committees and workshops, requested and issued reports, and worked with industry to develop self-regulatory codes of conduct. It conducted "sweeps" of both child-directed and general audience Web sites to assess information practices, and encouraged stakeholders to engage in their own research to document privacy practices on the Internet, which led to additional surveys of business practices online and consumer expectations about them. And it employed its bully pulpit power to call for credible self-regulatory efforts.

These methods led to the development of a detailed public record of factual data about privacy-impacting technologies and related business practices, and how these practices in turn related to consumers' expectations and privacy concerns. This—combined with the enactment by forty-six state legislatures, beginning with California's in 2002, of legislation requiring notification to affected parties of security breaches involving personal information (National Conference of State Legislatures 2010)—greatly increased the transparency of corporate privacy practices, the invisibility of which had left them largely immune to regulatory, media, and market pressures, and shielded them from sustained public debate.

The FTC's participatory fora provided a well-resourced space for that debate, existing agency privacy expertise, and relatively high-profile opportunities for advocates to shape the discourse about corporate data practices. Workshops accorded an opportunity for advocacy organizations to consolidate communication about privacy concerns faced by an otherwise diffuse consumer population and to convey their views to a powerful DC audience that included the press, congressional staff, trade associations, lobbyists, and industry executives.

Together, these developments led to a new understanding about the meaning of privacy as a trade practice shared across the privacy field—a substantive understanding that privacy should protect consumers' expectations about the flow of personal information, even in circumstances in which firms might have formally provided notice to those consumers and received their consent in a manner recognizable by contract law. In contrast to the static requirements and prohibitions of U.S. sectoral statutes, then, the FTC's activities fostered an evolving set of privacy norms as the agency, in conjunction with the cadre of experts empowered by its activities, took advantage of the breadth of its "unfair and deceptive" practices authority to shape the terms of the debate in a dynamic fashion.

The evolving consumer-oriented notion of privacy protection, moreover, underlies the threat of formal enforcement. This occurs in two ways. First, the agency increasingly uses its roving enforcement power to selectively push at boundaries, targeting, publicizing and identifying practices it deems "unfair" and transactions that were on the whole misleading despite legal disclosures. Second, the FTC permits advocates to file complaints requesting investigations of corporate privacy practices. Through a compelling FTC complaint, an advocacy organization can both leverage the resources of a formidable agency and generate significant publicity, trigging broader scrutiny of corporate practices. The level of advocate complaints this has generated augments the private attorney general function significantly, as it contrasts starkly with the far more costly realm of litigation in which privacy-protection organizations have rarely led court challenges to remedy privacy wrongs in the corporate sector. Together, these enforcement elements have contributed to a growing imprecision about what it meant to satisfy the measures of "privacy protection" and "consumer expectations." They have unraveled settled understandings of the agency's requirements regarding corporate privacy practices and focused industry instead on understanding and respecting evolving and context-dependent norms as they seek to deploy new technologies, new information practices, and new business models.

IV. CORPORATE PRIVACY PRACTICES UNDER THE SHADOW OF NEW GOVERNANCE

In considering the turn to new forms in of governance in privacy context, we have engaged in a wide-ranging project to collect empirical information, both

qualitative and quantitative, documenting privacy's operationalization "on the ground" (Bamberger and Mulligan 2011). The earliest evidence of internal corporate best practices developed in the "shadow" of new governance—derived from semistructured qualitative interviews with nine Chief Privacy Officers (CPOs) identified as field leaders, as well as from internal organizational charts, process documentation, and discussions with managers responsible for policy implementation—is presented below.[2]

The subset of privacy professionals interviewed 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. In choosing this method of identification, then, we sought out those leaders and firms to whom others in the field look when ascertaining best practices.

Our respondents came from firms that were heterogeneous on every metric except size—all but one was a Fortune 1000 company. The firms included those both governed by sector-specific privacy statutes, and from unregulated sectors; those both global in scope, and only domestic; and those both with highly diversified business lines, and with a single industry focus. Those interviewed had varied personal characteristics; some were lawyers and others had operational or technical expertise. A number had worked in government, while most had exclusively private-sector careers.

Yet, in discussing the importance of new methods of governance our respondents spoke with striking uniformity both about the relevance of new governance approaches in shaping their approaches to privacy and about the privacy management structures that resulted.

A. NEW GOVERNANCE ON THE CORPORATE RADAR: EXTERNAL DRIVERS OF PRIVACY PRACTICES

If new forms of governance have played little role in the dominant scholarly literature on privacy regulation, they loom large in the accounts of the privacy officers we interviewed (Bamberger and Mulligan 2011).

While respondents mentioned the need to comply with specific privacy-directed statutory schemes, they also indicated that such measures played a limited part in shaping their understanding of what "privacy" demanded of corporate actors. While specific compliance rules needed to be codified into overall corporate systems so that they are never breached, one explained, "the law in privacy will only get you so far." As to many things that "privacy" requires, said another, "there's no law that says 'you have to do this.' " Thus, specific laws, in the words of one CPO, "enforce the minimum"; then, another continued "we build from there."

By contrast, respondents uniformly identified new forms of privacy governance as key external drivers in framing their efforts at privacy protection.

Respondents cited particular FTC actions and other "FTC governance-type issues" as instigators for their firms' decisions about the allocation of resources to their privacy leadership function. They described the threat of FTC oversight as a motivating "Three-Mile Island" scenario and a catalyst for "good dialogue" with regulators. The FTC's "loose framework" explained a fourth, provides an "extra layer" that "I don't think any privacy officer wants to skirt with. . . . You have to analyze that in terms of the strict compliance line versus what can we do above and beyond that that's appropriate." Thus, another summarized, 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."

Several described, moreover, the ways in which the FTC's activities, combined with the effects of the breach notification laws, strengthened the position of the privacy function within their firms, indicating that the "fear aspect or . . . the risk aspect" was a far more effective driver for allocation of resources than "an appeal to the . . . greater good." As another described, "it was the FTC oversight [of other firms] and the length of scrutiny and the cost of audit that they had to submit to that I think was the dollar lever that started to open that box for me." Similarly, news reports from breaches at other organizations provided CPOs externally driven opportunities to summarize and circulate "lessons learned" from each incident, and help justify expenditures for implementing new protocols within their own organizations. In the words of one respondent, "the breach news . . . was so loud that it didn't take much to get the attention of our senior executive on data security, kind of as part of the privacy program." Another reported, "[the security breach laws] enriched my role; it's putting more of an emphasis on leadership internally in a very operational sense."

Finally, the interviewed privacy leaders' understandings of privacy reflected the language resonant in the legal "field," defined by legal sociologist Lauren Edelman (2007) as "the environment within which legal institutions and legal actors interact and in which conceptions of legality and compliance evolve" (58). Specifically, privacy was framed in terms of the substantive consumer-expectations approach emerging in the FTC's workshops, statements, and enforcement actions, and in the advocacy of many privacy activists (Bamberger and Mulligan 2011). The environmental uncertainty this evolving standard engendered, moreover, was central to belief in the necessity of a dynamic, forward-looking outlook towards privacy, in the place of a rules-compliance approach. "[I]t's more than just statutory and regulatory," described one CPO, "it's such an evolving area." As one summarized, "We're really defining [privacy as] 'looking around corners.' "

B. OPERATIONALIZING PRIVACY: STRUCTURES WITHIN THE CORPORATION

New governance scholars suggest the promise of approaches that both exploit regulatory ambiguity and harness a combination of state, market,

and private forces to create ongoing and multifaceted external stimuli on corporate actors. Such external forces are intended to both spur and enlist the judgment and expertise of those inside firms to organize themselves in ways that best pursue the integration of public goals into corporate decision making and to do so in a way that eschews one-time fixes in favor of dynamic and experimentalist problem solving. Given the salience of new governance approaches to the corporate understandings of privacy, then, what internal practices and structures have been adopted in their shadow?

Our interviews with privacy leaders, in concert with the examination of internal documents from the firms they serve, revealed a dynamic and layered architecture of corporate privacy decision making. The nine corporations whose CPOs we interviewed actively manage privacy concerns within the firm. The firms uniformly have overarching privacy policies, which are published and publicized, which govern the approach to privacy across business unit and jurisdiction, and which guide and inform both strategic decisions and day-to-day practices. They coordinate activities to send signals about the centrality of privacy to the firm's core goals such as company-wide "Privacy Days" and other training and awareness-raising educational programs. They dedicate significant resources to integrating individuals responsible for privacy in strategic decision making at multiple levels in the corporate structure.

Our respondents, moreover, described two characteristic features extant in some form in each of their firms. First, there was a powerful and relatively autonomous professional privacy officer at the top level of firm management, whose job includes substantial engagement with external stakeholders. Second, architectures were intended to distribute privacy decision making throughout firm units, notably by (1) including privacy in existing risk management processes and (2) by embedding privacy decision making within business-unit structures—both by placing accountability for setting and meeting privacy objectives on high-level business-unit managers and by integrating a network of specially trained employees into business lines as a means of identifying and addressing privacy concerns during the design phase of business development.

1. Privacy Leadership from the Top: The Role of the CPO

The development of the corporate CPO offers the most ready evidence of sea change in privacy management. In the late 1990s, companies in the financial and health sectors began creating CPO positions (Brown 2002). By 2000, companies in other sectors created CPO positions as well—often to great fanfare, as evidenced by numerous press releases announcing the appointments (Bamberger and Mulligan 2011). Already by 2005, moreover, CPOs at half of the Fortune 500 companies were directors or c-level executives (Poneman Institute 2005). Today, the International Association of Privacy Professionals (IAPP) claims 6,500 members.

Our interviews add depth to the portrait of leaders in this professional group and the ways in which their power, function, and role reflects the new governance elements of the regime in which they function. In particular, the interviews pointed to several key elements of this role: the centrality of the CPO's location within the corporate structure and its policy-making autonomy, as well as the way in which external engagement shapes the substantive focus of the CPO role.

a. The Structure of the CPO: Location and Autonomy

If the press "drumbeat" the "fear aspect" of enforcement, and the linkage between privacy and consumer behavior placed privacy concerns on the corporate radar, the location within the corporate structure of the privacy leads we interviewed reflects a centrality accorded to the privacy function. Each was either located within the c-suite or reported directly to a c-level executive. Several reported directly to the chief executive officer (CEO), while others had less direct but nonetheless significant reporting structures, such as one who reports to a strategic vice president, and another who "ha[s] a dotted line to the CIO, a dotted line to the chief compliance officer and a solid line up to the general counsel." Every firm, moreover, had instituted some form of formal reporting of privacy issues to the corporation's board of directors, and many of the CPOss we interviewed described substantial interaction with board subcommittees, or the body as a whole. "Either I or somebody makes a presentation around the privacy-related thing every time [the board] meet[s]" described one interviewee, while in another firm, "[t]hey tend to hear about privacy probably three or four or maybe half a dozen times a year." Thus, because "data management inside the company [. . .] has enormous implications [as] to how effectively we're going to manage the privacy of our customer's information[,] it's talked about at very, very senior levels . . . [including] presentations to the audit committee and board of directors on where we're at with privacy."

More subjectively, along with their location in the upper echelons of corporate management, respondents described the professional deference they were accorded in developing approaches to privacy. Such a phenomenon would not be surprising. Organizational scholars have long pointed to the importance professionalism has as an important institution for mediating uncertainty in the face of environmental ambiguity (Edelman 1992; Arrow 1963), and explored the ways in which individuals important to shaping access and control to necessary external resources—like legal legitimacy—become increasingly powerful internal firm decision makers (Pfeffer and Salancik 1978).

Indeed, the interviews explicitly make the connection between the development of a norm-dependent, contextual, socially driven conception of privacy in the wider legal field and their own professional autonomy. Top executives recognize the centrality of privacy protection; in the words of one

CPO, "privacy is to the information age what the environment was to the industrial age. You know, it's our big impact on our environment to misuse data in a way that environmental resources were misused earlier in the industrial age. And we'll be paying this cost if we don't get this right now. . . . The data Valdez." Another described the effect of regulator criticism of what firm executives had assumed were sufficient privacy practices as "similar to, you know, a nuclear warhead being dropped." Thus, "the company has this almost insatiable, undescribed vision" about privacy.

Yet the dynamic, multifaceted nature of privacy pressures obscures clear solutions for top managers, because "the rules change," because "[c]ustomer expectation changes," because the "bar changes and it's different by industry and it's different by moment in time," and because "the regulations or even the perception of the public changes."

CPOs consistently linked this uncertainty to the wide latitude accorded them to define and structure their organizations' privacy agendas at both the policy and implementation levels. "[T]ypically," one explained, "your boss [doesn't] have a good . . . 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."

b. The External Orientation of the Strategic CPO

Our respondents further described the way their own roles had developed in the light of the latitude accorded top privacy professionals. CPOs described their roles and responsibilities as heavily strategic, as opposed to operational or compliance oriented. Their function, one described, was "to take a much more forward look" aimed at identifying "solutions that we could think about to develop that are not even on perhaps the drawing board right now." They sought processes by which they no longer had to "rely on the development process to catch [privacy issues]" because the firm structures were designed "to understand how to do this with privacy built in right from the onset." Accordingly, CPOs reported spending substantial portions of their time on strategic planning—"looking over our priorities, understanding where our business is going and the kinds of privacy related issues or challenges that we either face or will face."

They describe the ways that the location of the CPO function within the corporate structure facilitates this strategic role internally. It permits participation in high-level strategic decision making and ensures that privacy concerns are integrated in strategic firm decisions rather than addressed as an "add-on"—or never considered at all. One CPO speaking about inclusion in high-level conversations stated, "I liken it to going up to the bridge of Starship Enterprise and hanging out. Big picture thinking, CEO thinking." CPOs reported extensive participation in formal leadership committees that establish firm strategy. Participation in such committees was viewed as a source of internal power positioning privacy as a strategic consideration in a

wide range of business decisions. "The fact that I sit on the . . . Chief Executive Council with all the GCs, means I get to hear about new programs," described one CPO; "And just also having the privacy leader sitting there at these meetings means people go, 'Oh, yeah. I wonder if there's a privacy aspect to this.'" Thus, from the very highest levels, CPOs discussed the importance of integrating privacy concerns throughout decision making about firm goals, products, and services by ensuring a privacy voice at the table—a tactic reflected as well by the practice of placing of employees responsible for privacy throughout operational units, discussed below.

The very uncertainty about the external environment governing privacy that enhances CPOs' stature, autonomy, and strategic role within the firm, however, complicates their privacy management task; in the words of one, "we're all still learning."

Because this uncertainty results from the interplay between norms, technical and business changes, and flexible regulatory authority to mediate between the two, CPOs say, such learning requires deep and ongoing external engagement. The CPOs thus all described substantial interactions with external stakeholders including regulators and civil society. For each, somewhere between a third and half of their job focuses on external engagement. This engagement, moreover, was distinct from lobbying, which, if engaged in, was carried out by other firm participants, albeit with substantive CPO input.

Such an outward orientation is essential, many explained, for guiding appropriate internal firm behavior. "I don't think you can be a good privacy officer without knowing the external environment," said one, "I really don't." This knowledge was cited as an essential source of input to the CPO's professional judgment, as well as a source of power within the firm. As another described,

> Not only can you then come back to the organization and say what you think is important and here is why, and here's how other companies tackled it, but you can also help strain that, shape it, and go work with policies makers, etc. Absolutely critical, you've got to spend a significant amount of time outside the organization.

The CPOs discussed their ongoing engagement with regulators, ranging from relationship building, to education, to prebriefings. One CPO, for example, described "go[ing] door to door . . . to maintain good relationships with [privacy regulators], and be part of the kind of dialogue about global privacy." Others discussed regular interactions with the FTC and privacy advocacy groups in which they aired contemplated policy changes and new products and services, seeking feedback. Another discussed a two-day meeting to educate a specific regulatory agency about the mismatch between the privacy regulations and the firm's business model in an effort to identify substantively equivalent models for compliance. And, of course, the CPOs interviewed participated in numerous legislative and regulatory hearings and agency-sponsored workshops.

Finally, 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. All but one of the privacy leaders we interviewed played a leadership role in the IAPP. The association's publication and dissemination of information as to best-practices approaches and its capacity to provide a space for "networking" and "getting to see the other privacy offers," one respondent said, is about getting "drenched in the culture." They also reported participation in multistakeholder initiatives focused on advancing privacy in various contexts outside the regulatory sphere. Some report bringing external privacy stakeholders—such as members of advocacy organizations, academics, and former regulators—into the firm to increase their own and the larger firms understanding of privacy. They all participate in conferences and workshops that bring multiple privacy perspectives to the table, such as the IAPP annual conference, the annual international conference of privacy and data protection commissioners, Computers Freedom and Privacy, and the Privacy Law Scholars Conference. Participation in the external privacy discourse through both informal and formal interactions assists CPOs in becoming "drenched in the culture" of privacy in ways that fosters intuition as to privacy sensitivities in the face of new risks and contexts.

The external presence of the CPO, to be sure, may have additional strategic significance. Several firms represented in our sample have run afoul of privacy norms (facing regulatory action, litigation, or other forms of substantial pushback). Yet their CPOs were nonetheless viewed by a cross-section of stakeholders as leaders in the profession; a companies' past fidelity to privacy expectations was clearly not a litmus test for future leadership. This suggests that perhaps the firm's legitimacy within the privacy community—including privacy regulators—should be influenced by external manifestations of privacy management distinct from specific privacy outcomes. This proposition seems particularly apt here, where what privacy requires of firms today may be quite distinct from what it requires tomorrow despite the absence of new formal rules. Where consistency with external norms is a primary source of legitimacy, yet its achievement is elusive due to their changing nature, the visibility of the CPO may reflect a form of "institutional isomorphism" (DiMaggio and Powell 1983, 150), serving an important function in signaling effort and engagement to external stakeholders even in the face of substantive privacy failures. The public-facing activities of the CPO identifies a firm as aspiring to legitimate social practices, even if it may fail to meet them in practice.

Regardless of motivations—which are undoubtedly mixed—the role of the CPO as described by our respondents involves a dual orientation. On the one hand, they engage in behavior gauging the privacy climate, sharing information about firm policies and practices, and participating in the privacy discourse. On the other, they use that information to shape internal

corporate strategy at a high level, translating it for deployment within the firm.

2. Operationalizing Privacy throughout the Firm

While our interviews explored the leadership aspects of the CPOs' roles, they also described a variety of ways in which privacy has been operationalized across and downward in the firm. These fall, roughly, into two categories. First, they involve the leveraging of existing risk management functions as a means of aligning privacy with other core firm goals. Second, they involve distributing expertise—through embedded experts, training, decisional tools, and the assignment of accountability—throughout firm business units.

a. Leveraging Core Firm Processes: A Strategic Risk Management Focus

To the extent the nature of privacy governance requires a dynamic, "learning," approach, many of our respondents described, privacy is increasingly framed as part of the evolving practice of risk management. "[W]e're all talking about risk," said one interviewee, "And how do we mitigate risk at the same time we're . . . protecting information."

Such a risk management focus, accordingly, has permitted privacy's inclusion in enterprise-wide governance activities, including enterprise risk management and audit, which CPOs viewed as significant for several reasons. Some emphasized this phenomenon as a means for adding privacy to the list of issues considered in setting the overall policy and strategic direction of the firm. "[T]he real sort of policy governance is going to happen . . . [at] the enterprise risk management policy group. . . . I'm in that group, our head of IT security is in that group; we have an ethics compliance and a risk officer in that group."

In addition to the substantive and strategic value of inclusion, many noted that such integration made greater resources available to each issue through economies of scale. For example, one CPO discussed the adoption of a single "fundamental governance model" establishing a "compliance process, an oversight process . . . a risk-management [process]" and a crisis-management process that was applied across privacy and other disciplines. The CPO noted that this integration was valuable because it built a process and architecture that would be expensive if pursued independently and also explained that that the use of a consistent process across risk categories reduced the overhead on the business units. Similarly, the CPO discussed privacy red flags included in the technology system that tracked every product and process, from creation to production. Just as individual workers were required, at various junctures, to sign off on questions intended to flag production, cost, performance, and other operational risks—which would then be exposed and highlighted for the relevant managers to address—so were they asked questions to determine whether the product-implicated concerns related to the treatment of personal information.

A second CPO discussed "an inspection readiness toolkit that helps [business units] implement the policies" across the firm and the use of server configurations to establish and maintain marketing preferences. Several others discussed the use of access controls to manage access to personal information, while still others pointed to "product lifecycle" management tools that provide a "deep understanding of what that data is that goes on the systems" during product development.

While a component of overall risk management, moreover, CPOs have leveraged the resources and attention available for both information privacy and information security by additional integration of their risk management activities. "[T]he way that we've even approached an organizational risk management," summarized one CPO, "is merging security and privacy together." CPOs reported close collaboration with chief information security officers, including joint management committees, regular meetings, joint educational and audit activities, and other informal and formal means of integration. Other CPOs discussed the ways in which the integration of privacy and security concerns permitted the allocation of resources for special crossing-cutting standing committees, initiatives to consider risks of specific new initiatives, and short-term task forces.

Finally, in every firm we considered, treating privacy as a manageable risk permitted privacy officers to profit from system-wide audit activities, including those reported to the board. Two firms, moreover, reported regular external privacy audits. The CPOs discussed their participation in defining the set of auditable criteria and the role this plays in affirming business-line accountability on privacy metrics. CPOs reported audits of privacy training goals, business design documentation, and customer preference management among other subjects.

Many CPOs conveyed a sense of achievement in having won a seat for privacy at the audit table. "[W]e've worked to make privacy reviews a part of every single internal audit," one explained. In the assessment of another, integrating an auditing function was "probably the most significant move" they accomplished—"we have four full-time privacy auditors." CPOs indicated the utility of audits in focusing the attention of senior executives within business units. In one CPO's opinion, "[internal] auditing changed everything." Explaining the significance of audits in establishing accountability, another CPO stated, "audit identifies the issue, gets management to agree on a set of action plans, they're documented, published, and my oversight role . . . is to make sure that . . . those action plans are realistic, that they're not missing what we really do, and then quite frankly make sure that it's being followed up."

b. Distributed Expertise and Accountability

The harnessing of effective audit and risk management capacity is particularly important to the privacy officers we interviewed because of the way it

facilitates a separate aspect of privacy's operationalizion. Specifically, every CPO we interviewed described internal privacy structures that relied on a distributed network of privacy professionals and specially trained employees within the different business units, enabled with practices and tools that assist with identifying and addressing privacy during the design phase of business development.

As our interviewees describe, this distributed form of privacy management takes a number of forms and is designed to further multiple goals.

It begins with the collaborative development of policies and practices. Authority for setting high-level policy about the corporation's goals and commitments regarding, and guidelines for the treatment of personal information, rests with subject-matter experts under the CPO's direct authority. Yet business-line executives are directly involved in the development of the specific privacy policies and practices that will govern their domain. While dedicated privacy officers, together with the legal team, often conduct the initial drafting, the privacy leaders we interviewed all viewed meaningful business-unit participation, as well as feedback from other functional areas, such as security or enterprise risk management, as important to ensure "buy in." In one firm, the CPO described, "we will consult with lines of business that are affected by those aspects of the policy we're reviewing. And we'll say 'Review this, tell us whether it does everything you need it to do.' " Another described a model by which privacy policies were developed by "a cross-functional team that had representation from all of the lines of business."

The engagement of the business unit in policy development and implementation, in turn, establishes the basis for holding business-line executives accountable for achieving privacy goals. Indeed, the majority of the firms at which our interviewees worked situated primary accountability for privacy with senior executives in the business units, in the same way that they are responsible for core measures, such as productivity and profits. Describing how such distributed accountability works in action, one CPO explained,

> if there is an issue . . . it's the accountability of the vice-president of marketing, not of me. You know, my role is to help them understand what it is they have to do but then their role is the implementation so that accountability is very important for them to understand.

As another described, "my team is not responsible for compliance, they're responsible for enabling the compliance of the business," and "if what we hear is bad, I'd say . . . 'Go audit these people.' "

The privacy leaders we interviewed considered such policies holding business-line executives responsible essential to the success of privacy management within the firm because of the weight that this direct line of accountability carries within the corporation. As one described it, "the executive management saying they're accountable is, I think, very powerful." In

describing this power, another analogized it to their experience in sending out a privacy survey:

> We [the office of the CPO] sent out 90 surveys, we got 7 responses. Once the guys who wrote them the check sent out the surveys, we got 98 responses . . . isn't that special!

As another explained more directly,

> [Y]ou know, their own executive directors or VPs in that area will say, "Now, why are we doing this? Because we don't really see the benefit of this activity." And so they can speak with that authority that you can't as a privacy office, you know? They don't give you credibility and say you know the business but, when their own executives look at it and you help them understand the privacy risk, then they look at that and say, "You know, it's not really worth it to do that."

Beyond the drafting of policies and the assignment of accountability, the critical method for the distribution of the privacy function throughout the firm involved "embedding" employees responsible for privacy management within business units and empowering them through a mix of privacy decisional tools, technical decision-guidance mechanisms, and business-unit appropriate training. These responsible employees—personnel with a variety of training and expertise in privacy, who may or may not handle privacy issues full time—offer privacy officers a means for expanding both the depth and breadth of privacy's "tentacles" within the organization. One firm whose CPO we interviewed, for example, employed twenty people "fully dedicated to privacy," but three hundred more who worked on the issue globally, through relevant business units. Another reported between thirty and forty full-time employees as well as four hundred part-time employees. A third reported approximately eighteen employees working full time on privacy management (not including privacy lawyers), with privacy focal points in each business unit at the senior executive level.

The structures for such embedded personnel vary by firm. The corporation with the most centralized structure assigns to specific business units privacy leads that report directly to the CPO. In this structure, the privacy leads were viewed as integral components of the business unit's decision-making process and took part in the design and rollout of new products and services. The CPO of this firm described "realigning my staff along the lines of supporting our business . . . match[ing] expertise, skill sets and /or interest" in an attempt to move the privacy orientation of the organization away from "a minimum reactive, late in the game" approach to a "strategic and best in class" approach.

Several other firms also have full-time privacy subject-matter experts in each business unit or product line, some with an overlay of privacy experts assigned to countries, geographic regions, or countries similarly situated with respect to stage of development, the firm's business interests, or types of risk.

However, unlike the first firm, these subject-matter experts often report directly within the business line and only indirectly to the CPO.

In still other instances, firms assigned a "lead" privacy expert, with a direct report to the CPO, to business units but further supplemented their privacy work with a range of second-tier employees responsible for privacy who report fully within the business unit itself. For example, as one CPO described, their corporation had "full-time people in each of the business units, and then we have" privacy advocates "that are embedded in each part of the business. So we have a requirement that there be a privacy lead in every single subsidiary, every single marketing organization." Another said, "I have privacy officers in each area that report to me on a dotted line but they're a solid line into their own business area. So they have a commercial—we have a marketing privacy officer and she has a dotted line to me and a solid line to the V.P. for marketing."

In each of these models, the embedded privacy staff engages in a variety of activities, depending upon their relative level of privacy expertise. At the low end, embedded privacy staff is used to identify issues for consideration by others acting as issue spotters or triage personnel. At the high end, they are full privacy professionals with responsibility for developing appropriate business-level policies through coordination with the CPO, other privacy professionals, and the business unit senior executives. In some organizations workflow and design documentation and technology are used heavily to provide "self-serve" privacy guidance to nonexperts making business-line decisions. For example, one firm utilizes a suite of self-help tools for the businesses to assist them in passing privacy "checkpoints" and a privacy impact assessment tool that integrates internal privacy requirements and external compliance issues into a dynamic set of questions based upon projects and data, the results of which are reported and audited. In others, by contrast, privacy documentation is used primarily to surface issues to be referred to experts rather than to direct their resolution.

Regardless of the nature of the reporting structure, the CPOs we interviewed viewed the functional embeddedness of privacy experts as enormously important for several reasons. The ability to leverage existing staff members within the business units by providing them with specialized training and decisional tools to assist them in surfacing privacy issues and identifying alternatives that reduce privacy risks was considered an important tool for positioning privacy as a design requirement rather than a legal matter—for "translating the world of privacy into regular business language." Moreover, the distributed system of expertise and tools allowed privacy, like other requirements, to be considered organically, from the start of a business-planning process; they are, in the words of one CPO, an invitation to "get engaged [with privacy] right in the outset, because the organization wants to understand how to do this where privacy is built in right from the onset."

The devolution of responsibility for privacy implementation and accountability, moreover, was cited as strategically important as a means to reorient the relationship between the privacy officers and the business units. As one CPO explained,

> [If] I had a 20-person group that all reported directly to me . . . I'd be imposing, I'd be demanding and imposing and, you know, cajoling. . . . [But in this decentralized structure] they're coming to me and saying, "Hey, you got to help us, you know, we're coming to privacy stuff, you've got to help us. I'm accountable for this but I'm not comfortable."

Another described the dynamic as follows:

> [It] was initially a lot of effort and work, now, thankfully, it's gone pretty native. So the questions that we get back from our marketers are much more sophisticated than, "Do I need to have a notice?"

And in the words of a third, "[It's] insinuating yourself further and further into the planning . . . So making sure that we're consulted."

V. EARLY ASSESSMENTS

Any assessments of these early findings must be tentative. Our inquiry focuses primarily on firm processes and structures rather than substantive privacy outcomes. Our sample is a limited one, including only nine industry leaders. And our qualitative data about the experiences and motivations of the CPO necessarily includes subjective accounts of parties reporting, in part, about their own roles.

Yet the potential salience of these developments and the promise they may offer for meaningful privacy management are highlighted through comparison with the state of corporate privacy management described in H. Jeff Smith's 1994 study (discussed in this article's introduction), and considered in light of the rich literature on corporate structure and organizational decision making.

A. SETTING A BASELINE: SMITH'S 1994 STUDY

The privacy practices documented in Smith's study arose in a governance context markedly distinct from that which exists today in several key respects. On the one hand, as he described, privacy problems were largely invisible to those outside the corporation. Several of those he interviewed put a sharp point on the connection between such external invisibility and internal inattention to privacy. "After all," said one, "if a customer's information is revealed inappropriately, who really knows about it?" (85) In the words of another,

> I hate to say "what they don't know won't hurt them," but that's really how I see it. If we buy personal information . . . or pull some from another database, there's never any way the customers will know about it . . . they won't ever be able to figure out . . . how can they complain? (88)

And, as a third admitted, "some of the things that are done with customers' information would make them angry . . . if they knew about it" (89).

On the other hand, Smith noted, firms received little ongoing regulatory oversight. In the absence of ongoing pressure, executives eschewed any responsibility based in their superior knowledge or position in the information society to proactively identify and address privacy issues. Aside from complying with laws prescribing corporate behavior, executives felt their duty was to maintain maximum flexibility over data use to ensure profitability.

Smith found that the processes of privacy management developed in this environment were remarkably similar among the seven firms he studied. And he documented shortcomings in corporate privacy management along four related dimensions, each reflecting structural deficiencies within the firm.

First, and most fundamental, he found a "wandering and reactive" policy-making process (55), with "large holes in privacy policies" and "numerous gaps" between policies and organizational practices (93). He attributed these shortcomings to the lack of "forceful, voluntary leadership," as executives avoided responsibility for an ill-defined and ambiguous task that was conceptually at odds with general corporate goals (56). The lack of top-level policy vision, he described, led to piecemeal adoption of practices by mid-level managers.

Second, consistent with this last assessment, Smith described the disengagement of privacy practices from considerations of "societal expectations" with respect to use of personal information (97). Public engagement was shunned, as both futile and unrewarding. In the words of one executive, "When others define for me what is 'ethical,' I will be ethical. Until then, I will make money" (91).

Third, Smith recorded a focus on short-term benefits of "organizational efficiency and effectiveness" rather than longer-term strategic aspects of personal information management (85). He attributed this to the failure express privacy as a core firm goal through integrated policies and practices to guide mid-level managers facing questions about new uses of personal information or deployments of technology in the context of day-to-day decision making. Privacy was therefore viewed as a "beyond compliance" add-on that hindered firm efficiency and for which no one in his or her right mind would seek out responsibility.

Finally, and relatedly, Smith documented employee discomfort with organizational decisions about the use of personal information flowing from the failure of firms to provide a vocabulary for, and a structure for acting upon, privacy concerns encountered in firm practices. These failures, he found, led managers and employees to sublimate their privacy concerns, resulting in missed opportunities to address privacy issues as they arose.

B. IDENTIFYING PROGRESS

Salient elements of the governance context in which Smith conducted his study have changed dramatically. The combined activities of a multitude of players in the privacy field, as well as the disclosure requirements of the breach notification laws, have increased the visibility of privacy practices and intensified the external forces pressuring corporations. And the contrast between Smith's study and our respondents' account of corporate practice in the shadow of such new governance phenomena is striking.

On the most basic level, the privacy leaders we interviewed described the substitution of proactive and strategic privacy management in place of Smith's "wandering and reactive" policy-making process. CPOs are integrated into senior management. These executives promulgate policies and practices intended to manage privacy cohesively and consistently throughout the firm. Such mechanisms in turn send powerful signals about the importance of privacy to the members of the firm as a whole. These developments alone are worth notice, as they provide the indicia of strong management commitment—in the form of "corporate policies, organizational structure, measurement and control systems . . . and organizational culture" (Murray 1976, 7)—shown to improve implementation of firm changes intended to satisfy external mandates (Greening and Gray 1994; Stevens, Beyer, and Trice 1980; Murray 1976) and promote the fulfillment, and even improvement beyond, compliance standards (Kagan, Gunningham, and Thornton 2003; Fox-Wolfgramm, Boal, and Hunt 1998). Centralized coordination of issues across business units, moreover, can help ensure that these issues are not marginalized and avoid "silo" behavior in which locations and divisions are principally focused on maximizing their own accomplishments, harming the organization as a whole (O'Dell and Grayson 1998; Gioia and Thomas 1996).

In a variety of more complex ways, moreover, the developments we describe suggest important mechanisms for overcoming firms' resistance to external efforts to reorder internal priorities, a problem described in the rich literature on organizational decision making. This scholarship demonstrates that firms are structured to foster the pursuit of preexisting interests, and "institutional arrangements constrain options and establish the very criteria by which people discuss their preferences" (Kagan, Gunningham, and Thornton 2003, 89). Yet, it also identifies methods for reorienting firm behavior and altering entrenched cognitive frames and processes, a number of which appear to be at work in the privacy area, specifically reflected by the CPO's role in bringing outside emphases on privacy into corporate norms and the architectures by which those norms are then disseminated across the firm.

1. The Boundary-Spanning CPO

First is the inclusion in the CPO role of an external, in addition to its internal, orientation. Today, the corporate privacy focus is not tethered to

compliance, but rather tied to a broader "license to operate" (Kagan, Gunningham, and Thornton 2003, 76) that includes issues of legality, market pressures, and significantly concerns of social actors and is "interactive," "open to interpretation, negotiation," and "amendment" (Kagan, Gunningham, and Thornton 2003, 77). This new orientation places ethics and social obligations—as defined by noncorporate actors—within the scope of firm consideration. Here they inclined CPOs to ask whether the firm's activities were "creepy" or could be defended in the media or to "friends and family," rather than simply defend them as legally permissible.

Neil Gunningham, Robert Kagan, and Dorothy Thornton (2004) have identified the manner in which internal perceptions and attitudes of management "act as an important filter through which information about the external licenses is sifted and guided" (325), and having a high-level executive engaged in this process can offer a tool for improving decision making within the firm in several important ways. Participation in the external privacy discourse can assist in developing a CPO's own judgment as to the state of external demands on a corporation. Research on decision making in the face of uncertainty reveals the primacy of deep knowledge of substance, people, and institutions—as well as past events and solution spaces—to the development and exercise of expertise and the rapid intuitive decision making at its core (Lipshitz, Klein, Orasanu, and Salas 2001; Eraut 2000; Klein 1993). A sustained presence in the ongoing negotiations about the meaning of privacy and its enforcement can permit the acquisition of the tacit knowledge and expertise to address new privacy issues in high-stakes, time pressured situations. Moreover, a decision maker's exposure to ways of thinking outside of a particular organization and interaction with others whose thought processes are not governed by the same culture or "knowledge structures" (Heath, Larrick, and Klayman 1998, 20; Walsh 1995, 291) can be an especially powerful means for changing a decision maker's information environment. Accordingly, such exposure provides a powerful means of learning and for preventing the ossification of routinized ways of approaching problems.

Direct engagement with the privacy claims and justificatory frameworks of external stakeholders may in turn promote more effective decision making within the firm, as CPOs—high-level insiders—bring into the firm perspectives of other organizations negotiating privacy externally. This facet of the CPO's job is of great significance because of the connection between the legitimacy of firm behavior and proper intuiting of evolving privacy norms that, unlike prescriptive rules, are dynamic, are at times contradictory, can diverge both up and down from the law on the books, and vary contextually (Dowling and Pfeffer 1975). The forums, workshops, reports, and other informal policy-making venues at the FTC, as well as shared-learning events run by the IAPP, advocates, and academics, support the sharing of diverse expertise and insight across sectors of the privacy community. In such environments of interorganizational collaboration, "[l]earning takes place as a transformation of exploration between organizations to exploration within

the single organization" (Holmkvist 2003, 112). By this process, engagement with other organizations can effect intrafirm changes, as "[t]he organization internalizes what has been jointly explored with other organizations" (ibid.). As such, a CPO can play an important "boundary-spanning" role (Bamberger 2006, 452), serving both as a voice for privacy and as a trusted insider and using a "privacy mindset" to spur mindful internal decision making in the face of pressure to focus on efficiency and profit.

2. Distributive Architectures: Integration, Empowerment, and Accountability

Second, the developments our respondents describe suggest several important tools for better integrating privacy as a core firm value in the face of competing corporate goals and for harnessing the skills, expertise, and intuition of those employees Smith found disempowered and suffering " 'emotional dissonance' as they struggled to reconcile two competing values" as a result of "polices [that] were either nonexistent or inconsistent with present practices" (Smith 1994, 86).

Sim Sitkin and Robert Bies (1993) contrast the effect of organizational rules that are easily included in the existing chain of command with those that violate routinized order and the chain of command—the former, not surprisingly, yield a far higher incidence of success. While Smith's study described a landscape in which privacy compliance rules created profound tensions with other firm goals, our respondents described their assimilation into existing management processes. Incorporating privacy measures into other risk management systems, they explained, both harnessed significant resources in the service of privacy and put the treatment of information privacy on a level with other fundamental management concerns. The involvement of senior business-unit executives in establishing tailored policy and implementation plans, and assignment of accountability to them, accordingly heightens the seriousness with which employees consider privacy. The CPOs' participation in high-level strategy-setting fora provides a voice for privacy in setting firm priorities. And blending privacy into business-unit decision making from the start offers a means for transforming privacy from a cost or limit to a function that must be integrated into each product or service along with other core specifications.

Organizational theorists like Lawrence and Lorsch (1967) argue that a decentralized decision-making structure provides the most effective response to an uncertain external environment—such as exists here in the demands for corporate treatment of privacy—because it permits individuals who are closest to the problem to react and make better-informed decisions. The development of a distributed network of experts empowered with training materials and decisional tools focuses on bringing such expertise into firm processes organically and meaningfully. The distribution of privacy expertise throughout the firm can be viewed as an effort, like the integration of privacy into risk management discussed above, to avoid around the siloing of

external impacts along functional lines. Institutional theory considers professions to be key carriers of ideas among and across institutional fields (DiMaggio and Powell 1983). By embedding privacy experts and empowering business-unit employees with greater privacy, knowledge firms are building receptors sensitive to privacy inputs into components of the organization with no natural inclination to either feel or respond to such stimuli. This distributed architecture, then, seeks to leverage the normative commitments handed down by the CPO with experiential expertise drawn from context.

Here, moreover, such decentralization is combined with additional measures directed to fostering effective decision making both by individuals and by the corporate structure of which they are a part. The attention of both business-unit executives and the privacy staff included within the business-unit structures is directed towards privacy—it is a subject that they "own" and for which they bear responsibility. Yet, their roles in privacy decision making are not prescribed from above. The expertise of unit leaders as to how privacy should be integrated successfully into existing workflows and decision structures is enlisted in a manner that respects unit leaders' autonomy, which has been shown to improve outcomes (Marcus 1988). Preserving managerial autonomy in a way that frames the achievement of goals as an opportunity rather than a threat fosters commitment to implementation of policies (Sharma 2000)—policies that, after all, those managers themselves helped create and champion.

Both formal firm policies assigning responsibility to business-unit executives, moreover, and the decisional tools provided to other employees charged with a privacy role within business units, make those individuals aware of privacy choices for which they are held personally accountable. Research has found that such accountability signals the importance of the task and fosters a sense of responsibility for surfacing information about risks, whatever the competing factors (Argyris 1994). Individuals assigned accountability for a decision are more likely to engage in more analytic and complex judgment strategies (Tetlock 1985; McAllister, Mitchell, and Beach 1979) and take more care in making decisions (Schwartz and Wallin 2002). The benefits of accountability in promoting meaningful decision making are pronounced especially in contexts—as here—in which those assigning accountability do not have set views as to the correct solution.

Finally, the value of the distributed architectures that our respondents described is underscored by Smith's identification of the privacy-minded but disempowered individuals in the firms he studied. The policies, training, and decisional tools provided to employees within the firms we studied both provide a language to discuss privacy and require employees across the firm to engage with the privacy impact of their design choices, business strategies, and information flows. Thus, this corporate infrastructure provides privacy-minded employees with a language to express their concerns, a bully pulpit from which to speak, and an audience of senior personnel awaiting the surfacing of privacy red flags from below. For those less privacy-minded,

these same tools provide a periodic reminder to focus on privacy, pulling them out of their standard decision-making processes and focusing them on privacy at various stages of work. These tools may both help employees navigate the changing privacy landscape in a manner that alleviates cognitive dissonance and provide communication structures that surface rather than mask "the kinds of deep and potentially threatening or embarrassing information" that leads to organizational learning and change (Argyris 1994, 78).

VI. CONCLUSION

New governance approaches suggest the use of collaboration, education, and legal ambiguity both to make firms more permeable to external demands and to enlist their expertise regarding the achievement of public goals in particular corporate contexts. By these criteria, the interview accounts of nine corporate privacy leaders suggest some measure of success.

They describe privacy's operationalization through both the activities of a high-level privacy officer and a distributed network of privacy professionals and specially trained business-line employees, capacitated with practices and tools that assist with identifying and addressing privacy during the design phase of business development. These distributed mechanisms extend the reach of the CPO into the firm, facilitating both the downstream communication of privacy objectives and the disclosure and escalation within the firm of privacy risks. The integration of privacy into existing decision-making structures, moreover, promotes privacy's consideration as a systemic risk, consistent practices across firm units, and the commitment of employees from across the firm.

This architecture ensures that Chief Privacy Officers (CPOs) determine the substance of privacy policy, but also engage business units in defining and tailoring privacy protection within specific corporate environments. But it also allocates responsibility for compliance with business-aligned privacy objectives to senior executives within each unit.

Finally, it reflects the increasing reliance on new approaches to privacy governance and the fact that corporate privacy activities must respond to evolving, and multiple, external norms and demands. As such, it requires CPOs to span boundaries—regularly engaging with external participants to shape and understand privacy's evolving definition, and to reflect external perspectives on privacy in firm norms and practices. In contrast to the situation last documented fifteen years ago, in which corporate privacy practices were characterized by invisibility and disengagement, these interviews suggest proactive engagement with stakeholders, a heightened willingness to expose practices and policies to preadoption scrutiny, and engaged participation in defining privacy's aims and requirements. By these accounts, then, privacy within the firm has moved out of the closet and become a strategic concern, while, simultaneously, firms have been called onto the public stage

to engage in a dialogue about the role of privacy in modern life and what it requires of organizations seeking a "social license" to operate.

NOTES

1. Federal Trade Commission Act (FTC Act) 15 USC § 45 (a)(1) (1976) (prohibiting unfair and deceptive acts or practices in or affecting commerce, commonly referred to as the FTC's Section 5 jurisdiction).
2. Initial interviews, running an hour and a half to two and a quarter hours, were conducted primarily in person during 2007 and 2008, with follow-up interviews in 2009 and 2010. Most initial interviews took place in conference rooms at the offices of the interviewee or at off-site locations at the preference of the interviewee; two were conducted by phone but were otherwise identical. Questionnaires were used to collect biographical data about the interviewees and organizational information about the firm. Follow-up interviews were conducted in person, by telephone, and over email, and collected additional information about on-going corporate practices and procedures. In some cases policies and practices were shared, in other instances we were walked through materials—including employee training materials—remotely over the Internet.

KENNETH A. BAMBERGER *is Professor of Law at the University of California, Berkeley. His expertise involves the roles of public and private actors in regulation, technology in governance, and corporate compliance. He teaches courses in Administrative Law, Constitutional Law, and law and technology.*

DEIRDRE K. MULLIGAN *is an Assistant Professor in the School of Information at the University of California, Berkeley, where she is also a Faculty Director of the Berkeley Center for Law and Technology. Her research focuses on issues of information privacy, information security, surveillance and the interplay between legal rules and technical systems. She is the Policy Lead for the National Science Foundation's TRUST Science and Technology Center, Chair of the Board of the Center for Democracy and Technology, and Co-chair of Microsoft's Trustworthy Computing Academic Advisory Board.*

REFERENCES

Argyris, Chris. 1994. "Good Communication that Blocks Learning," *Harvard Business Review* 72 (4): 77–85.

Arrow, Kenneth J. 1963. "Uncertainty and the Welfare Economics of Medical Care," *American Economic Review* 53: 941–73.

Ayres, Ian, and John Braithwaite. 1992. *Responsive Regulation: Transcending the Deregulation Debate*. New York: Oxford Univ. Press.

Bamberger, Kenneth A. 2006. "Regulation as Delegation: Private Firms, Decision-making, and Accountability in the Administrative State," *Duke Law Journal* 56: 377–468.

Bamberger, Kenneth A., and Deirdre K. Mulligan. 2011. "Privacy on the Books and on the Ground," *Stanford Law Review* 63: 247–315.

Black, Julia. 2005. "The Emergence of Risk Based Regulation and the New Public Management in the UK," *Public Law* 512–49.

Brown, Christopher. 2002. Survey Finds Increasing Number of Firms Appointing Officers with Institutional Clout, 1 PRIV. & SECURITY LAW REPT. 78.

Center for Democracy & Technology. 2010. Introduction. *CDT's Guide to Online Privacy.* http://www.cdt.org/privacy/guide (accessed July 22, 2011).

Clinton, William J., and Albert Gore, Jr. 1997. *A Framework for Global Electronic Commerce.* Washington, DC: White House.

Coglianese, Cary. 2001. "Is Consensus an Appropriate Basis for Regulatory Policy?" In *Environmental Contracts: Comparative Approaches to Regulatory Innovation in the United States and Europe*, edited by Eric W. Orts and Kurt Deketelaere, 93–113. The Hague: Kluwer Law.

De Búrca, Gráinne, and Joanne Scott. 2006. "Introduction: New Governance, Law, and Constitutionalism." In *Law and New Governance in the EU and the US*, edited by Gráinne de Búrca and Joanne Scott, 1–14. Portland, OR: Hart Publishing.

DiMaggio, Paul J., and Walter W. Powell. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American Sociological Review* 48: 147–60.

Dorf, Michael C., and Charles F. Sabel. 1998. "A Constitution of Democratic Experimentalism," *Columbia Law Review* 98: 267–473.

Dowling, J., and J. Pfeffer. 1975. "Organisational Legitimacy: Social Values and Organisational Behaviour," *Pacific Sociological Review* 18 (1): 122–36.

Edelman, Lauren B. 1992. "Legal Ambiguity and Symbolic Structures: Organizational Mediation of Civil Rights Law," *American Journal of Sociology* 97: 1531–76.

---. 2007. "Overlapping Fields and Constructed Legalities: The Endogeneity of Law." In *Private Equity, Corporate Governance and the Dynamics of Capital Market Regulation*, edited by Justin O'Brien, 55–90. London: Imperial College Press.

Eraut, Michael R. 2000. "Non-Formal Learning and Tacit Knowledge in Professional Work," *British Journal of Educational Psychology* 70 (1): 113–36.

Federal Trade Commission. 1996. Staff Report. *Consumer Privacy on the Global Information Infrastructure.* Washington, DC: Federal Trade Commission.

---. 1999. *Self-Regulation and Privacy Online, Prepared Statement of the Federal Trade Commission, presented by Chairman Robert Pitofsky before the Subcommittee on Communications of the Committee on Commerce, Science, and Transportation, United States Senate July 27, 1999.* Washington, DC: Federal Trade Commission.

Fligstein, Neil. 1991. "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*, edited by Walter W. Powell and Paul J. DiMaggio, 311–36. Chicago: Univ. of Chicago Press.

Fox-Wolfgramm, Susan J., Kimberly B. Boal, and James G. Hunt. 1998. "Organizational Adaptation to Institutional Change: A Comparative Study of First-Order Change in Prospector and Defender Banks," *Administrative Science Quarterly* 43: 87–126.

Gioia, D. A., and J. B. Thomas. 1996. "Identity, Image and Issue Interpretation: Sensemaking during Strategic Change in Academia," *Administrative Science Quarterly* 41: 370–403.

Greening, D., and B. Gray. 1994. "Testing a Model of Organizational Response to Social and Political Issues," *Academy of Management Journal* 37 (3): 467–98.

Gunningham, Neil, Robert A. Kagan, and Dorothy Thornton, 2004. "Social License and Environmental Protection: Why Businesses Go Beyond Compliance," *Law & Social Inquiry*, 29: 307–41.

Heath, Chip, Richard P. Larrick, and Joshua Klayman. 1998. "Cognitive Repairs: How Organizational Practices Can Compensate for Individual Shortcomings," *Research in Organizational Behavior* 20: 1–37.

Hetcher, Steven. 2000. "The FTC as Internet Privacy Norm Entrepreneur," *Vanderbilt Law Review* 53: 2041–62.

Holmkvist, Mikael. 2003. "A Dynamic Model of Intra- and Interorganizational Learning," *Organization Studies* 24: 95–123.

Hoofnagle, Chris Jay. 2005. *Privacy Self-Regulation: A Decade of Disappointment.* Washington, DC: Electronic Privacy Information Center. http://epic.org/reports/decadedisappoint.pdf (accessed July 22, 2011).

Kagan, Robert, Neil Gunningham, and Dorothy Thornton. 2003. "Explaining Corporate Environmental Performance: How Does Regulation Matter?" *Law and Society Review* 37: 1–90.

Karkkainen, Bradley C., Archon Fung, and Charles Sabel. 2001. "After Backyard Environmentalism: Toward a Performance-Based Regime of Environmental Regulation," *American Behavioral Scientist* 44: 692–709.

Klein, Gary A. 1993. "A Recognition-Primed Decision (PRD) Model of Rapid Decision Making." In *Decision Making in Action: Models and Methods*, edited by Gary A. Klein, Judith Orasanu, and Robert Caldenwood, 138–47. Norwood, CT: Ablex Publishing.

Lawrence, P. R., and Jay W. Lorsch. 1967. *Organization and Environment.* Boston: Graduate School of Business Administration, Harvard Univ.

Lipshitz, R., G. Klein, J. Orasanu, and E. Salas. 2001. "Taking Stock of Naturalistic Decision Making," *Journal of Behavioral Decision Making* 14: 331–52.

Lobel, Orly. 2003. "Orchestrated Experimentalism in the Regulation of Work," *Michigan Law Review* 101 (6): 2146–62.

---. 2004. "The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought," *Minnesota Law Review* 89: 342–55.

March, James G., and Herbert A. Simon. 1958. *Organizations.* New York: Wiley.

Marcus, Alfred A. 1988. "Implementing Externally Induced Innovations: A Comparison of Rule-Bound and Autonomous Approaches," *Academy of Management Journal* 31 (2): 235–56.

McAllister, P. W., T. R. Mitchell, and L. R. Beach. 1979. "The Contingency Model for the Selection of Decision Strategies," *Organizational Behavior and Human Performance* 24: 228–44.

Merton, Robert K. 1957. *Social Theory and Social Structure.* Glencoe, IL: Free Press.

Murray, Jr., Edwin A. 1976. *The Academy of Management Review* 1 (3): 5–15.

National Conference of State Legislatures. 2010. *State Security Breach Notification Laws.* http://www.ncsl.org/default.aspx?tabid=13489 (accessed July 22, 2011).

O'Dell, Carla, and C. Jackson Grayson. 1998. "If Only We Knew What We Know: Identification and Transfer of Internal Best Practices," *California Management Review* 40 (3): 154–75.

Poneman Institute. 2005. *Privacy Professional's Role, Function and Salary Survey Report.*

Pfeffer, Jeffrey, and Gerald R. Salancik. 1978. *The External Control of Organizations: A Resource Dependence Perspective.* New York: Harper & Row.

Rakoff, Todd D. 2000. "The Choice between Formal and Informal Modes of Administrative Regulation," *Administrative Law Review* 52: 159–74.

Reidenberg, Joel R. 1999. "Restoring Americans' Privacy in Electronic Commerce," *Berkeley Technology Law Journal* 14 (2): 771–92.

Rotenberg, Marc. 2001. "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)," *Stanford Technology Law Review* 1: http://stlr.stanford.edu/STLR/Articles/01_STLR_1.

Rubin, Edward L. 2005. "Images of Organizations and Consequences of Regulation," *Theoretical Inquiries in Law* 6 (2): 347–90.
Sabel, Charles F., and William Simon. 2004. "Destabilization Rights: How Public Law Litigation Succeeds," *Harvard Law Review* 117: 1015–101.
Salancik, Gerald R., Jeffrey Pfeffer, and J. Patrick Kelly. 1978. "A Contingency Model of Influence in Organizational Decision Making," *Pacific Sociological Review* 21: 239–56.
Schwartz, Paul M. 1999. "Privacy and Democracy in Cyberspace," *Vanderbilt Law Review* 52: 1609–702.
Schwartz, Steven T., and David E. Wallin. 2002. "Behavioral Implications of Information Systems on Disclosure Fraud," *Behavioral Research in Accounting* 14: 197–221.
Sharma, S. 2000. "Managerial Interpretations and Organizational Context as Predictors of Corporate Choice of Environmental Strategy," *Academy of Management Journal* 43: 681–97.
Sitkin, Sim B., and Robert J. Bies. 1993. "The Legalistic Organization: Definitions, Dimensions and Dilemmas," *Organization Science* 4: 345–51.
Smith, H. Jeff. 1994. *Managing Privacy: Information Technology and Corporate America*. Chapel Hill: Univ. of North Carolina Press.
Stevens, John M., Janice M. Beyer, and Harrison M. Trice. 1980. "Managerial Receptivity and Implementation of Policies," *Journal of Management* 6: 33–54.
Sunstein, Cass R. 1991. "Administrative Substance," *Duke Law Journal* 40: 607–46.
---. 1999. "Informational Regulation and Informational Standing: Akins and Beyond," *University of Pennsylvania Law Review* 147: 613–75.
Sturm, Susan. 2001. "Second Generation Employment Discrimination: A Structural Approach," *Columbia Law Review* 101: 458–60.
Tetlock, P. E. 1985. "Accountability: The Neglected Social Context of Judgment and Choice." In *Research in Organizational Behavior*, vol. 7, edited by L. L. Cummings and B. M. Staw, 297–332. Greenwich, CT: JAI Press.
Trubek, Louise G. 2002. "Public Interest Lawyers and New Governance: Advocating for Healthcare," *Wisconsin Law Review* 2002: 575–601.
Walsh, James P. 1995. "Managerial and Organizational Cognition: Notes from a Trip Down Memory Lane," *Organization Science* 6 (3): 280–321.