Privacy in Europe: Initial Data on Governance Choices and Corporate Practices

Kenneth A. Bamberger & Deirdre K. Mulligan

Forthcoming, *George Washington Law Review* (August 2013)

Privacy in Europe: Initial Data on Governance Choices and Corporate Practices

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

ABSTRACT

As this article goes to press, the European Union is embroiled in debates over the contours of a proposed new privacy regulation.

These efforts, however, have lacked critical information necessary for reform. For they—like privacy debates generally—focus almost entirely on law "on the books"—legal texts enacted by legislatures or promulgated by agencies.

By contrast, they largely ignore privacy "on the ground"—the ways in which corporations in different countries have operationalized privacy protection in the light of divergent formal laws, different approaches taken local administrative agencies, and other jurisdiction-specific social, cultural, and legal forces.

Indeed, despite the new regulation's central goal of harmonizing privacy across Europe by preempting today's enormous variation in national approach, policymakers have been hobbled by an absence of

[*] Professor of Law, University of California, Berkeley; Faculty Director, Berkeley Center for Law and Technology.

[**] Assistant Professor, University of California, Berkeley, School of Information; Faculty Director, Berkeley Center for Law and Technology.

This project has received generous support from: the Berkeley Center for Law and Technology, including funds from a Nokia Corporation research grant; the Miller Institute for Global Challenges and the Law at Berkeley Law; the Privacy Projects.org; the Intel Corporation; the Rose Foundation for Communities and the Environment Consumer Privacy Rights Fund; and TRUST (the Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422).

We are also extremely grateful for assistance in developing this project from Jen King, David Thaw, and Chris Hoofnagle; for critical assistance in Europe from Pascale Gelly, Francoise Gilbert, Christoph Klug, Marcos Judel Meléndrez, Fabrice Naftalski, Omer Tene, Eduardo Ustaran, Stewart Dresner and Privacy Laws and Business, Trevor Hughes, Rita DiAntonio and the International Association of Privacy Professionals, and Ulrich Wuermeling and Euroforum; for feedback from commentator Dennis Hirsch, organizers Chris Hoofnagle and Dan Solove, and others at the 2013 Privacy Law Scholars Conference; and participants at International Association of Privacy Professionals 2013 conferences in Washington and London, at the Ernst & Young/Microsoft/IAPP December 2012 KnowledgeNet in Paris, and at the Fall 2012 conference of the Section on Administrative Law and Regulation of the ABA; and for excellent research support from Hailey Anderson, Emily Barabas, Marta Porwit Czajkowska, Nathalie David-Warcholak, April Elliot, Heather Ford, Kim Fox, Ilan Goldbard, Lea Mekhneche, Alisha Montoro, Mary Morshed, Parichart Munsgool, Celia Perry, Sarah Ruby, Quinn Shean, Tatyana Shmygol, Sara Terheggen, James Wang, Andy Wiener, and Cory Isaacson Zinn.

August 2013 Vol. 81 No. 5

evidence as to which national choices about privacy governance have proven more or less resilient in the face of radical technological and social change. Information about the relative strengths and benefits of the alternate regulatory approaches that have flourished in the "living laboratories" of the European member states is largely undeveloped.

This Article begins to fill this gap—and at a critical juncture. Our "on the ground" project uses qualitative empirical inquiry—including interviews with, and questionnaires completed by, corporate privacy officers, regulators, and other actors within the privacy field in three European countries, France, Germany and Spain, to identify the ways in which privacy protection is implemented in different jurisdictions, and the combination of social, market, and regulatory forces that drive these choices. It thus offers a comparative "in-the-wild" assessment of the effects of the different regulatory approaches adopted by these three countries.

In the face of novel challenges to privacy, leveraging the adaptability of distinct regulatory approaches and institutions has never been more important. As technological and social change has altered the generation and use of data, the definition of privacy that has prevailed in the political sphere—individual control over the disclosure and use of personal information—has increasingly lost its salience. In particular, the common instruments of protection generated by this definition—procedural mechanisms to protect individual "choice"—have offered an inapt paradigm for privacy protection in the face of data ubiquity and computing capacity. In developing new metrics for protecting privacy, policymakers must take into account a far more granular, and bottom-up, analysis of both differences in national practice and the forces on the ground that result in the diffusion—or lack thereof—of corporate structures and institutions that research suggests are most adaptive in protecting privacy in the face of change.

Through such comparative analysis, this Article upends the terms of the prevailing policy debate, revealing the ways that different regulatory choices have shaped corporate behavior.

It offers important insights for policymakers considering reform not just in Europe, but also in United States, where Congress, the Federal Trade Commission, and the Obama administration have all expressed a willingness to reexamine deeply the current regulatory structure, and a desire for new models.

And, more broadly, it underscores the importance of administrative agencies' choices about regulatory tools and approaches, relations with those that they regulate, and their own internal structures, in shaping the *mindset and behavior of the private firms they govern to maximize public values.*

TABLE OF CONTENTS

INTRODUCTION

Privacy governance is at a crossroads. In light of the digital explosion, policymakers in North America and Europe have commenced a wholesale process of revisiting regulation of the corporate treatment of information privacy. The recent thirtieth anniversary celebration of the Organization for Economic Cooperation and Development's ("OECD") *Guidelines on* *the Protection of Privacy and Transborder Flows of Personal Data*,[1] the first international statement of Fair Information Practice Principles ("FIPPs"), sparked an international review of the Guidelines to identify areas ripe for revision.[2] National data privacy regulators reviewing the European Union ("E.U.") Data Protection Directive have, in turn, suggested alternative regulatory models oriented around outcomes.[3] The European Commission is actively debating the terms of a new Privacy Regulation.[4] Congress, the Federal Trade Commission ("FTC"), and the current U.S. presidential administration have signaled a commitment to deep reexamination of the current regulatory structure and a desire for new models.[5]

These efforts, however, have lacked critical information necessary for reform. Scholarship and advocacy around privacy regulation has focused almost entirely on law "on the books"[6]—legal texts enacted by legislatures or promulgated by agencies. By contrast, the debate has surprisingly ignored privacy "on the ground"[7]—the ways in which corporations in different countries have operationalized privacy protection in the light of divergent formal laws, decisions made by local administrative agencies, and other jurisdiction-specific social, cultural, and legal forces.

With the exception of a 1994 study that examined the practices of

---

[1] Org. for Econ. Cooperation and Dev. [OECD], *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD Doc. C (80) 58 Final (Sept. 23, 1980) [hereinafter *OECD Privacy Guidelines*].

[2] *See The 30th Anniversary of the OECD Privacy Guidelines*, OECD, www.oecd.org/sti/privacyanniversary (last visited June 1, 2013).

[3] *See, e.g.*, NEIL ROBINSON ET AL., RAND EUR., REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE 47–49 (2009) (study commissioned by the U.K. Information Commissioner's Office).

[4] *See, e.g.*, Konrad Lischka & Christian Stöcker, *Data Protection: All You Need to Know about the EU Privacy Debate*, SPIEGEL ONLINE (Jan. 18, 2013, 10:15 AM), http://www.spiegel.de/international/europe/the-european-union-closes-in-on-data-privacy-legislation-a-877973.html.

[5] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 1–5 (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf; Adam Popescu, *Congress Sets Sights On Fixing Privacy Rights*, READWRITE (Jan. 18, 2013), http://readwrite.com/2013/01/18/new-congress-privacy-agenda-unvelied; Edward Wyatt, *F.T.C. and White House Push for Online Privacy Laws*, N.Y. TIMES, May 10, 2012, at B8.

[6] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 260 (2011) [hereinafter Bamberger & Mulligan, *Privacy on the Books*].

[7] *Id.* at 249.

seven U.S. companies,[8] no sustained inquiry has been conducted into how corporations actually manage privacy in the shadow of formal legal mandates.[9] Moreover, no one has ever engaged in a comparative inquiry of corporate privacy practices across jurisdictions. Indeed, despite wide international variation in approach, even the last detailed comparative account of different countries' enforcement practices occurred over two decades ago.[10] Thus, policy reform efforts progress largely without a real understanding of the ways in which previous regulatory attempts have actually promoted, or thwarted, privacy's protection.[11]

This Article is the third in a series documenting a project intended to fill this gap—and at a critical juncture. The project uses qualitative empirical inquiry—including interviews with and surveys of corporate privacy officers, regulators, and other actors within the privacy field—to identify the ways in which privacy protection is implemented on the ground, and the combination of social, market, and regulatory forces that drive these choices. It also offers a comparative analysis of the effects of different regulatory approaches adopted by several OECD nations, taking advantage of the living laboratory created by variations in national implementation of data protection, an environment that can support comparative, "in-the-wild" assessments of the ongoing efficacy and appropriateness of these policies.

While the first two Articles in this series discussed research documenting privacy implementation in the United States,[12] this Article presents the first analysis of data of its kind from Europe. The analysis stems from research and interviews in three E.U. jurisdictions: Germany, Spain, and France.

This Article reflects only the first take at this recently-gathered data; the analysis is not comprehensive, and the lessons drawn at this stage are necessarily tentative. A complete consideration of the research on the privacy experience in five countries (the United States, Germany, France, Spain, and the United Kingdom) will appear in an upcoming book-length

---

8 *See* H. JEFF SMITH, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA 15–17 (1994).

9 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 249.

10 This was a study of privacy in several North American and European countries. DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES (1989).

11 *See infra* notes 114–119 and accompanying text.

12 *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry*, 33 LAW & POL'Y 477 (2011) [hereinafter Bamberger & Mulligan, *New Governance*]; Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6.

treatment.[13]

Yet this Article offers as-yet unavailable data about the European privacy landscape at a critical juncture—the moment at which policymakers are engaged in important decisions about which regulatory structures to expand to all E.U. member states and which to leave behind.[14] Policymakers must also consider how those individual states will structure the administrative agencies governing data privacy moving forward, the strategies those agencies will adopt regarding legal enforcement, the development of expertise within both the government and firms, and the ways that other participants within the privacy "field"[15] will (or will not) be enlisted to shape corporate decisionmaking and privacy outcomes.

Setting up the context for this analysis, Part I of this Article describes the dominant narratives regarding the regulation of privacy in the United States and the European Union—accounts that have occupied privacy scholarship and advocacy for over a decade.[16] They portray a U.S. regulatory regime characterized by a patchwork of weak, incomplete, and fractured privacy statutes, the absence of an agency dedicated to data protection, and a consequent lack of clear guidance, oversight, and enforcement.[17] They also describe a U.S. privacy framework that fails to provide across-the-board procedures that empower individuals to control the use and dissemination of their personal information.[18]

By contrast, these narratives herald a "European" model of protection:

---

13 Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Ground: Governance Choices and Corporate Practice in the US and Europe (forthcoming 2014) [hereinafter Bamberger & Mulligan, Privacy on the Ground] (drawing lessons for broader research on paradigms for thinking about privacy, the effectiveness of corporate practices informed by those paradigms, and organizational compliance with different forms of regulation and other external norms more generally).

14 *See* Lischka & Stöcker, *supra* note 4.

15 *See* Lauren B. Edelman, *Overlapping Fields and Constructed Legalities: The Endogeneity of Law*, *in* Private Equity, Corporate Governance and the Dynamics of Capital Market Regulation 58 (Justin O'Brien ed., 2007) ("[O]rganisational fields are understood as the environment within which organisations interact and in which conceptions of . . .legality and compliance evolve."); Paul J. DiMaggio & Walter W. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, 48 Am. Soc. Rev. 147, 148 (1983) ("By organizational field we mean those organizations that, in the aggregate, constitute a recognized area of institutional life: key suppliers, resource and product consumers, regulatory agencies, and other organizations that produce similar services or products.").

16 *See, e.g.*, Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 Ind. L. Rev. 173, 179 (1999) (analyzing conflicts between the United States and the European Union over data privacy).

17 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 258–60.

18 *Id.* at 256–60.

omnibus FIPPs-based[19] privacy principles in law or binding codes, interpreted and monitored by an independent and dedicated privacy agency.[20] While they differ in detail, reform proposals generally concur that increasing corporate attention and resources devoted to privacy and improving substantive privacy outcomes in the United States requires the convergence with such a model.[21]

These descriptions of the state of privacy law "on the books" are, in many ways, accurate.[22] However, they fail to capture even very basic attributes of the manner in which privacy regulation actually works in the jurisdictions they characterize—and the way that privacy governance and privacy practices have (or have not) proven adaptive in the face of technological and social change altering the generation and use of data.[23] Specifically, these accounts offer no explanation for the fact that—even without any changes in formal statutes—corporate privacy management in the United States has undergone a profound transformation. American corporations now commit relatively massive amounts of resources to privacy, as evidenced by the employment of chief privacy officers and other privacy professionals, privacy certification and training, new privacy practices in major law firms and audit firms, and the development of privacy seal and certification programs.[24] Even more fundamentally, they reflect that there is not just one "European" privacy regime, but many. Privacy implementation in Europe reflects major variation across jurisdictions, in terms of administrative structure and behavior, social discourse, and corporate behavior.[25]

Part II summarizes our project to develop more granular accounts of the privacy landscape, leading to the interviews presented in this Article, while Part III presents the findings of our previous scholarship investigating privacy "on the ground" in the United States. That work documents and evaluates an emerging framework for thinking about privacy as a matter of risk management and consumer trust rather than as

---

[19] FIPPs are central tenants of privacy protection that have been memorialized in many sources, including the OECD Guidelines. *OECD Privacy Guidelines*, *supra* note 1.

[20] *See infra* notes 47–49 and accompanying text.

[21] *See infra* notes 82–88 and accompanying text.

[22] Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 260.

[23] *Id.* at 251.

[24] *See id.*; *see also infra* notes 103–112 and accompanying text.

[25] *See infra* Part IV.A–C; *see also* ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 32–33, 94 (2008); Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, 26 MICH. J. INT'L L. 807, 827–30 (2005) [hereinafter Bignami, *Transgovernmental Networks*].

an individual right to be vindicated by processes that notify and seek consent from data subjects regarding the use of their personal information. It further describes resulting trends in the architecture of internal corporate privacy management, including the role of the corporate Chief Privacy Officer and the "operationalization" of privacy within corporate decisionmaking and risk management structures.

These developments reflect a suite of generative forces far beyond the detail of the national regulatory statutes that combine to shape privacy's regulatory "field." These forces include the rise of the FTC as an "activist" privacy regulator enlisting new governance strategies to shape the privacy debate, as well as nonprofit privacy and consumer advocates, the media, state data breach notification requirements, E.U. requirements governing international data transfers, and the rapid professionalization of privacy managers.[26] These developments also reflect approaches to data protection that information scholarship suggests might best protect individual privacy in the face of changing technological and business models, and that researchers propose as most successful in motivating firms to enact secondary mandates—here, the protection of privacy—alongside core operational goals.[27]

Informed by our previous findings, Part IV presents the results of our research regarding corporate perception and implementation of privacy requirements in three European jurisdictions, Germany, Spain, and France, and places them within the theoretical framework regarding emerging best practices in the United States. Not surprisingly for those familiar with privacy protection in Europe, these results reveal widely varying privacy landscapes, all within the formal governance of a single legal framework: the 1995 E.U. Privacy Directive.[28]

More striking, however, are the granular differences between the jurisdictions. Despite the divergence between Germany and the United States regarding both the language in which privacy is discussed and the particular mandates and institutions shaping privacy's governance, the architecture for privacy protection and decisionmaking within German firms bears considerable resemblance to the emerging best practices we identified in the United States—practices that reveal particular adaptivity and suitability for addressing new challenges of the digital age.[29] By contrast, the privacy models in Spain and France differ from the U.S.

26 *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 285; *infra* notes 103–112 and accompanying text.

27 Bamberger & Mulligan, *New Governance*, *supra* note 12, at 480.

28 Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

29 *See infra* Part IV.A.

structure, focusing on more formal data registration, use, and reporting requirements.[30] This focus appears to position expertise outside the firm, with the formal regulators, decreasing investment in internal privacy expertise and limiting the reach and power of internal privacy experts.

Part IV then seeks to understand the construction of the privacy "field" that shapes these differing country landscapes. This inquiry examines the details of national implementation of the E.U. directive, including the specificity and type of requirements placed on regulated parties, the use of ex ante guidance as opposed to prosecution and enforcement, and the content of regulations, with particular attention to the comparative focus on process-based as opposed to substantive mandates. It also explores the structure and approach of the relevant data protection agency, including the size and organization of the staff; the level to which they rely on technical and legal "experts" inside the agency, rather than inside the companies they regulate; the use of enforcement and inspections; and the manner in which regulators and firms generally interact. Our inquiry takes stock of factors beyond privacy regulation itself, such as other legal mandates, characteristic elements of national corporate structure, and societal factors, such as the roles of the media and other citizens, industry, labor, and professional organizations that determine the "social license" that governs a corporation's freedom to act.

Finally, Part V outlines two elements of a new account of privacy's development, informed by comparative analysis. First, based on the data from four jurisdictions, it engages in a preliminary analysis regarding which elements of these privacy fields our interviews and other data suggest have fostered, catalyzed, and permitted the most adaptive responses in the face of novel challenges to privacy.[31] Particularly, this Part discusses the contribution of managerialization and nongovernmental actors to privacy protection. Second, Part V suggests something important about the diffusion of practices across jurisdictional lines in the face of important social and technological change. Specifically, it describes the ways in which variations in the timing of privacy's institutionalization in different countries permitted the development of new and adaptive forms of understanding and protecting privacy in the United States—the country whose institutions developed last—which have influenced emerging practices in European jurisdictions, notably through diffusion within professional networks.[32]

30 *See infra* Part IV.B–C.

31 *See infra* Part V.A.

32 *See infra* Part V.B.

With novel challenges to privacy, the adaptability of distinct regulatory approaches and institutions has never been more important. As technology and social change have altered the generation and use of data, the definition of privacy that has operated in the political sphere—individual control over the disclosure and use of personal information—has increasingly lost its salience.[33] In particular, the common instruments of protection generated by this definition—procedural mechanisms to ensure the perfection of individual choices—have offered an inapt paradigm for privacy protection in the face of data ubiquity and computing capacity.[34] Through a comparative analysis, this Article upends the terms of the prevailing policy debate, explores the capacity of different national regimes to respond to social and technological change and the ways that different regulatory choices have shaped corporate behavior, and offers important insights for policymakers considering reform.

I. RECONSIDERING NARRATIVES OF PRIVACY GOVERNANCE

A. Understanding Dominant Privacy Narratives

The foundation of information privacy protection throughout much of the world is "informational self-determination"[35] or "the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others."[36] This rights-based conception of information privacy is embodied in a set of FIPPs that provide the backbone for data protection laws in Europe and many other countries.

The OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, finalized three decades ago, provide an influential statement of FIPPs.[37] The Guidelines articulate eight principles "to harmonise national privacy legislation and, while upholding such human rights . . . at the same time prevent interruptions in international flows of

---

33 *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 148 (2010).

34 *Id.*

35 The term "informational self-determination" was set forth in a German court decision limiting the intrusiveness of the national census. *See* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, ENTSCHEIDUNGEN DES BUNDESVERFASSUNGSGERICHTS [BVERFGE] 65, 1984 (Ger.), *translated in* 5 HUM. RTS. L.J. 94, 97–101 (1984).

36 *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

37 *See OECD Privacy Guidelines*, *supra* note 1; *see also* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 101–11 (1992) (describing the OECD principles).

data."[38] These principles emphasize an individual's knowledge of, participation in, and control over personal information.[39] They embrace transparency regarding the types of information collected and the way the information will be used.[40] They propose certain limits on data collection—namely that "data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[41] They require data collectors to maintain information securely and emphasize the rights of data subjects to access and ensure the accuracy of personal information.[42] While a FIPPs approach is thus rooted in a commitment to the substantive principle of individual self-determination, it relies largely on procedural protections to support that principle, such as providing notice to the data subject and securing consent to informational use.[43]

Although this instrumental expression of privacy's value in a networked world spanned the Atlantic, it encountered dissimilar regulatory climates in the United States and Europe, and was, accordingly, implemented in divergent fashions. The account of this divergence has been the subject of significant scholarship, and has framed policy debates on both sides of the Atlantic.[44] By this narrative, the FIPPs framework resonated with national European Data Protection Authorities, some of which had existed since the 1970s,[45] and with existing frameworks of data protection, which echoed post-war commitments to privacy as an individual human right, animated by the experience of European fascism and totalitarianism.[46] The Privacy Directive adopted by the European

---

38 *OECD Privacy Guidelines*, *supra* note 1.

39 *See id.*

40 *See id.*

41 *Id.* ¶ 7.

42 Some FIPPs proponents consider such access rights to be "the most important privacy protection safeguard." BENNETT, *supra* note 37, at 103.

43 *See OECD Privacy Guidelines supra* note 1.

44 *See, e.g.*, Cate, *supra* note 16.

45 *See* NEWMAN, *supra* note 25, at 74–75 ("[T]he EU data privacy directive can be traced to its roots in the historical sequencing of national data privacy regulation and the role that the resulting independent regulatory authorities played in regional politics.").

46 *See* Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, Europ. T.S. No. 5 (affirming a right to general personal privacy); FRED H. CATE, PRIVACY IN THE INFORMATION AGE 43–44 (1997) (discussing the impact of the experience with Nazi Germany on European privacy laws); Omer Tene, *What Google Knows: Privacy And Internet Search Engines*, 2008 UTAH L. REV. 1433, 1460 ("The prohibition against secret databases is one of the doctrinal foundations of European privacy law, gleaned following decades of totalitarian regimes that used information in secret databases to police and terrorize citizens into conformity and submission.").

Union in 1995,[47] moreover, reflected the notion that a full implementation of the FIPPs approach's conception of data protection as a means of protecting individual rights requires comprehensive laws governing information collection and use regardless of type and sector, that are administered by a strong, single privacy enforcement authority that "knows exactly when to use the carrot and when to use the stick, and who is not concerned with balancing data protection with other administrative and political values."[48]

These elements of European privacy governance—omnibus protections reflecting a commitment to self-determination enforced uniformly by a dedicated privacy agency—typify what Abraham Newman has termed a "comprehensive" privacy regime.[49] Shaped in its detail by regulatory networks within Europe, it is an image of a privacy governance scheme that, as Newman describes, has spread globally through institutionalism by the European Union.[50] It has, moreover, served as the dominant metric against which the adequacy of U.S. regulation has been assessed.[51]

---

47 The directive provides an omnibus framework prohibiting the processing of personal data within the European Union in the absence of three conditions:

> (1) Pursuant to a transparency requirement, unless the processing of personal data is deemed "necessary" for a variety of articulated reasons (performing or entering a contract, compliance with a legal obligation or performance of a task carried out in the public interest, to protect the data subject's "vital interests," or for purposes of the legitimate interests of the party to whom the data are disclosed), it may occur only when the subject has given his or her consent. Subjects also have the right to be informed when personal data are being processed.
>
> (2 Personal data can only be processed for "specified, explicit and legitimate purposes" and may not be processed in a way incompatible with these purposes; and
>
> (3) Data processing and storage (including length of storage in a form that allows identification of data subjects) must be proportional to the purposes for which the data are collected.

See Council Directive 95/46, 1995 O.J. (L 281) 31 (EC). Pursuant to the Directive, moreover, personal data may only be transferred to parties in a third country if that country provides an "adequate level of protection." *Id.* While the U.S. regime has not been determined to meet that standard, a "safe harbor" framework developed by the Department of Commerce in consultation with the European Union Commission permits individual U.S. firms to self-certify their privacy practices, thereby allowing transfers of personal information from European countries. *See* Commission Decision 2000/520, 2000 O.J. (L 215) 7 (EC). For a description of the Safe Harbor Principles, see *U.S.-E.U. Safe Harbor Provisions*, EXPORT.GOV, http://www.export.gov/safeharbor/eu/index.asp (last visited June 2, 2013).

48 BENNETT, *supra* note 37, at 239 (describing the arguments of David H. Flaherty).

49 NEWMAN, *supra* note 25, at 23–24.

50 *Id.* at 36–37, 98–99.

51 *Id.* at 24.

In comparing the U.S. privacy framework to the European approach, critics have found the former lacking in many ways.[52] "[I]n contrast to the approach in many other nations," one scholar explains, "it is unusual in the United States to find any comprehensive privacy laws . . . that enumerate a complete set of rights and responsibilities for those who process personal data."[53] Rather, regulations in the United States target "specific, sectoral activities, such as credit reporting," health care, and electronic commerce.[54] Privacy is thus governed by numerous different laws administered by different government agencies, and sometimes no agency at all.[55] This scattered set of regulations treats privacy differently depending on the type of information involved and the sector in which it is used.[56]

The policies behind these statutes also vary considerably. Statutes such as the Fair Credit Reporting Act of 1970 ("FCRA"),[57] which regulates credit reporting,[58] and the Privacy Act of 1974,[59] which regulates collection and use of data by the federal government,[60] reflect the FIPPs' concept of "informational self-determination" and employ numerous safeguards,

---

52 *See* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 358 ("Privacy protection in the United States has often been criticized"). The United States has specifically been criticized for employing self-regulation. *See* Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes* 355 (N.Y.U. Sch. of Law. Pub. Law & Legal Theory Research Paper Series, Working Paper No. 10-16, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1510275 ("According to its many critics, privacy self-regulation is a failure. It suffers from an overall lack of transparency, weak or incomplete realization of Fair Information Practice Principles, inadequate incentives to ensure wide scale industry participation, and ineffective compliance and enforcement mechanisms.").

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

54 *Id.*

55 *See, e.g.*, 18 U.S.C. §§ 2510–2511 (2012) (extending restrictions against wiretaps to include transmissions of electronic data by computer); 18 U.S.C. § 2710(a)(4) (2012) (preventing disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual materials"); Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422 (2012) (protecting the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records).

56 *See, e.g.*, Gramm–Leach–Bliley Financial Modernization Act, 15 U.S.C. §§ 6801–6827 (2012) (empowering various agencies to promulgate data-security regulations for financial institutions); Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 42 U.S.C.) (regulating the use and disclosure of protected health information).

57 Fair Credit Reporting Act, 15 U.S.C. § 1681–81x (2012).

58 *Id.*

59 Privacy Act of 1974, 5 U.S.C. § 552a (2012).

60 *Id.*

including notice, information, and consent.[61] In contrast, more recent privacy measures have developed in response to the privacy concerns of consumers and threats to other interests.[62] These measures position privacy as an instrumental value that promotes other social goals. For example, "privacy laws might promote confidence in Internet commerce, with benefits both for surfers' privacy and companies' sales."[63] Early regulation of the Internet in the United States, which was characterized by limited government regulation and significant reliance on "self-regulation," reflects this instrumental approach.[64] In short, one scholar has described:

> [T]wo dominant models have emerged, reflecting two very different approaches to the control of information. The European Union . . . has enacted a sweeping data protection directive that imposes significant restrictions on most data collection, processing, dissemination, and storage activities, not only within Europe, but throughout the world if the data originates in a member state. The United States has taken a very different approach that extensively regulates government processing of data, while facilitating private, market-based initiatives to address private-sector data processing.[65]

This comparison has informed normative and descriptive assessments of privacy protection in a variety of ways. Most straightforwardly, it has undergirded a widespread and coherent critique of U.S. privacy regulation and resulting proposals for reform. Scholars, advocates, and politicians argue that the "patchwork"[66] nature of U.S. privacy laws leaves the United

[61] *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 257–58; *see also* Solove & Hoofnagle, *supra* note 52, at 357–62 (discussing the FCRA and Privacy Act of 1974 and explaining how "emerging companies known as 'commercial data brokers' have frequently slipped through the cracks" of these laws).

[62] Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 258.

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

[64] *See, e.g.*, THE WHITE HOUSE, THE FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE 4 (1997) (promoting self-regulation as the preferred approach to protecting online privacy); Rubinstein, *Privacy and Regulatory Innovation*, *supra* note 52, at 360 (explaining that the Clinton administration favored private sector leadership and supported self-regulation, believing it would help electronic commerce flourish).

[65] Cate, *supra* note 16, at 179.

[66] *See* Priscilla M. Regan, *Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows*, 59 J. SOC. ISSUES 263, 275 (2003) ("The patchwork of sectoral regulation . . . has long confused the Europeans"); *CDT's Guide to Online Privacy*, CTR. FOR DEMOCRACY & TECH. (Oct. 21, 2009) (discussing "[t]he existing motley patchwork of privacy laws and practices" in the United States); Larry Dignan, *Senate, Web Ad Titans Joust Over Behavioral Targeting*, BETWEEN THE LINES BLOG (July 9, 2008, 7:22 PM),

States with gaps in data coverage, confusion among regulated entities and consumers, and a tapestry of specific laws with limited ability to adapt to new technologies and business practices.[67] In many U.S. industries, consumers must depend on self-regulation to protect their private information without the assurances of government regulation or external incentives to encourage best practices.[68]

Further, critics comparing privacy approaches critique U.S. protections as "FIPPs-lite,"[69] a less robust approach than the FIPPs-based protections in European mandates.[70] They also contend that by supplying market-oriented rationales for privacy protection, the United States devalues "the moral weight of privacy"[71] and its role in a democratic society.[72]

---

http://blogs.zdnet.com/BTL/?p=9280 (quoting U.S. Senator Daniel K. Inouye as saying that "I fear that our existing patchwork of sector-specific privacy laws provides American consumers with virtually no protection.").

67 *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 258; Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶ 48 ("Technology continued to outpace the law. And the failure to adopt a comprehensive legal framework to safeguard privacy rights could jeopardize transborder data flows with Europe and other regions."). Neil M. Richards argues that patchwork laws in the United States "muddle" privacy and are inconsistent, pointing to the fact that "Facebook can disclose what music we listen to and what news articles we read, but not which films we watch" under the Video Privacy Protection Act. Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 702 (2013).

68 *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 258–59; Chris Jay Hoofnagle, *Privacy Self Regulation: A Decade of Disappointment*, ELECTRONIC PRIVACY INFO. CTR. (Mar. 4, 2005), http://epic.org/reports/decadedisappoint.pdf ("Ten years of self-regulation has led to serious failures in this field."); Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 775–76 (1999) (responding in part to THE WHITE HOUSE, *supra* note 64, critiquing U.S. reliance on self-regulation, and proposing FIPPS-based regulation).

69 *See Privacy Today: A Review of Current Issues*, PRIVACY RIGHTS CLEARINGHOUSE (2010), http://www.privacyrights.org/ar/Privacy-IssuesList.htm; *see also Federal Agency Protection of Privacy Act: Hearing on H.R. 4561 Before the Subcomm. on Commercial & Admin. Law of the H. Comm. on the Judiciary*, 107th Cong. (2002) (statement of Edmund Mierzwinski, Consumer Program Dir., National Association of State Public Interest Research Groups) (explaining that agencies have failed to strengthen their privacy policies in response to changes in technology).

70 Solove & Hoofnagle, *supra* note 52, at 358 ("Privacy experts have long suggested that information collection be consistent with Fair Information Practices.").

71 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 259.

72 *See* Schwartz, *Privacy and Democracy*, *supra* note 53, at 1682 (arguing that market solutions to privacy devalue the potential for cyberspace to facilitate "democratic self-rule"); *see also* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 500-01 (1995) (discussing privacy's role in "reflect[ing] specific conceptions of governance" in the public and private sectors); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560 (1995) (tying the "individual self-

The single attempt to engage in a sustained inquiry into how corporations actually manage privacy in light of U.S. regulation—conducted back in 1994—underscored these critiques.[73] That landmark study of privacy practices in seven firms, conducted by management scholar H. Jeff Smith, documented a privacy arena characterized by inattention and ambiguity.[74] In several important areas, privacy policies were nonexistent, and firms failed to follow those policies that did exist.[75] Executives did not treat privacy as a strategic corporate issue[76] and left privacy decisions to mid-level managers who lacked expertise and only responded to issues as they arose in practice.[77] Smith blamed the "ambiguity" of the American legal privacy regime for these problems.[78] In the face of this ambiguity, firms avoided action unless explicitly required by external parties, a trend that was further exacerbated by the general view that privacy goals conflicted with corporate operational aims.[79]

Accordingly, Smith concluded, remedying the problem of corporate inattention to privacy concerns required a "systemic fix."[80] The primary goal of new regulations, he argued, must be "the reduction of ambiguity in the U.S. privacy domain."[81] To attain this goal, Smith advocated a series of reforms, including many elements of the European approach to privacy protection.[82] He proposed a uniform set of principles along with a system for developing more individualized industry codes, based on FIPPs[83], an approach that emphasizes individual rights through requirements such as notice and consent, and he advocated for the creation of a governmental

determination" that privacy affords to society's capacity for democratic self-governance); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 734 (1987) ("[P]rivacy proves to be a prerequisite to the capacity to participate in social discourse. Where privacy is dismantled, both the chance for personal assessment of the political and societal process and the opportunity to develop and maintain a particular style of life fade.").

73 *See generally* SMITH, *supra* note 8.

74 *Id.* at 4, 137.

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

76 *Id.* at 4.

77 *Id.* at 9–13, 73, 82.

78 *See id.* at 139, 167–204 (describing "ambiguity all around").

79 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 250.

80 SMITH, *supra* note 8, at 207 (emphasis omitted).

81 *Id.* at 213.

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

83 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 250.

board to implement and enforce these new requirements.[84] According to Smith, this regime would be necessary to compel firms to make privacy protection a priority.[85]

Smith is not alone in his criticisms and suggestions. Scholars, advocates, industry leaders, and politicians have called for comprehensive legislation that follows FIPPs and includes agency oversight.[86] These potential resolutions rely on the normative notion that the current approach, especially in comparison to the E.U. model,[87] fails to protect privacy and must be changed to an "enforcement model of regulation," in which "Congress would define substantive privacy requirements for commercial firms based on FIPPs and authorize agency regulation as supplemented over time by court decisions interpreting their requirements."[88]

The accounts of divergent commitments and regulatory strategies between the United States and Europe have generally informed recent comparative law scholarship. One rich exploration of comparative privacy cultures begins with the observation that, although "[c]ontinental law is avidly protective of many kinds of 'privacy' in many realms of life . . . . [t]o people accustomed to the continental way of doing things, American law seems to tolerate relentless and brutal violations of privacy in all these areas of law."[89] Another scholar observed, "European and American citizens are caught between two very different, often clashing, legal cultures of privacy," concluding, "the difference is also one of basic values. Outside the core physical space of the home, Americans do not care particularly about privacy."[90]

---

84 *Id.*

85 SMITH, *supra* note 8, at 210.

86 *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 259; Consumer Privacy Legislative Forum, *Statement of Support in Principle for Comprehensive Consumer Privacy Legislation*, CTR. FOR DEMOCRACY & TECH. (June 20, 2006), http://www.cdt.org/privacy/20060620cplstatement.pdf (the signatories to this statement are Eastman Kodak Co., eBay Inc., Eli Lilly & Co., Google, Inc., Hewitt & Associates, Hewlett-Packard Co., Intel Corp., Microsoft Corp., Oracle Corp., Procter & Gamble Co., Sun Microsystems, Inc., and Symantec Corp).

87 The E.U. model articulates, in an "omnibus" fashion, certain uniform restrictions on the processing of personal data intended to promote the Fair Information Principles set forth by the OECD: *notice* to the subject and *consent* to data's use; *limits* on data's use to the purpose stated; data *security*; *disclosure* of information collection; *access* to one's data; and methods for holding data collectors *accountable*. *OECD Privacy Guidelines*, *supra* note 1. For a description of the E.U. Privacy Directive, see *supra* note 47.

88 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 259; Rubinstein, *supra* note 52, at 357.

89 James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L. J. 1151, 1156 (2004).

90 Bignami, *Transgovernmental Networks*, *supra* note 25, at 808.

This narrative has been extended in the significant recent comparative work by Priscilla Regan, Abraham Newman, and Francesca Bignami, which discusses the ways in which privacy law has evolved through institutions, networks, and regulatory diffusion.[91] Regan describes the ways in which "the E.U. as a state actor has played a forceful role," while "the United States as a state actor has played a largely reactive and passive role . . . in both the national and transnational debates" over privacy, which, she argues, undermines development of shared norms.[92]

Exploring beyond national boundaries, Newman and Bignami each develop accounts of privacy's comparative development that emphasize transnational networks, which, they argue, have resulted in a convergence of, and around, European regulatory forms.[93] In contrast to this emerging "European" model of privacy, they reject the notion that American approaches have had influence on global privacy governance.[94]

B. Cracks in the Dominant Narratives

The descriptive claims inherent in the dominant narratives regarding the comparative nature of U.S. and European privacy laws are in many ways accurate.[95] U.S. privacy laws are fragmented and depart frequently from a FIPPs understanding of the meaning of privacy, whereas European laws reflect a far greater commitment to comprehensive rules, dedicated administration, and notions of informational self-determination.[96]

Yet those narratives' central focus on legal and regulatory approaches as they exist "on the books" means that they overlook important elements in the privacy landscapes on both sides of the Atlantic. Indeed, they have failed to examine privacy "on the ground"—the way in which formal law, regulatory choices, and social forces shape the actual behavior of corporations tasked with protecting privacy.[97] Thus, despite the consistency of comparative narratives,[98] several important developments have suggested flaws in their accuracy.

---

91 *See* Regan, *supra* note 66; NEWMAN, *supra* note 25; Bignami, *Transgovernmental Networks*, *supra* note 25.

92 Regan, *supra* note 66, at 280.

93 *See* NEWMAN, *supra* note 25, at 2–3; Bignami, *Transgovernmental Networks*, *supra* note 25, at 809–10.

94 *See* NEWMAN, *supra* note 25, at 52, 73; Bignami, *Transgovernmental Networks*, *supra* note 25, at 809–10, 864.

95 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 260.

96 *See id.* at 256.

97 *Id.* at 249, 260; Lothar Determann, *Social Media Privacy: A Dozen Myths and Facts*, 2012 STAN. TECH. L. REV. 7, 9.

98 *See supra* notes 16–18 and accompanying text.

The first developments involve radical changes in the attention and resources dedicated to privacy protection in the United States. Smith's 1994 study of privacy "on the ground" documented the systemic inattention and lack of resources due to the incomplete and ambiguous nature of U.S. privacy laws and the absence of regulatory oversight.[99] Notably, executives did not consider privacy when making important decisions about technological and business developments[100]—as one mid-level manager recounts: "The top executives rarely ask for [privacy] policy implications of . . . new uses of information. If anybody worries about that, it's my [mid-level] colleagues and myself. And we don't usually know the right answer, we just try something."[101]

Yet by 2012, corporate privacy management in the United States had undergone a profound transformation. Numerous corporations have created chief privacy officer positions.[102] The International Association of Privacy Professionals ("IAPP"), a professional group dedicated to information privacy, boasts over 12,000 members[103] and offers information-privacy training and certification.[104] Privacy has also become a robust practice area in the legal field, as more companies search for expertise in privacy law.[105] PricewaterhouseCoopers and other firms offer privacy audits to companies seeking to ensure compliance with corporate

99 Smith, *supra* note 8, at 167–68, 212–13, 217–18.

100 *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 250.

101 SMITH, *supra* note 8, at 82.

102 *See* Press Release, Int'l Ass'n of Privacy Prof'ls, 2005 Ponemon Institute, IAPP Announce Results of Annual Salary Survey (Mar. 11, 2005), *available at* https://www.privacyassociation.org/about_iapp/media/2005_03_11_ponemon_institute_iapp_announce_results_of_annual_salary_survey ("[Fifty] percent of privacy professionals are at a director or higher level within their firms. [Eighty-four] percent report their position is a full-time ro[le] within their organization. [Forty-two] percent said their department has a direct line of report to a C-level executive within the organization, while [twenty-five] percent have a direct line of report to General Counsel.").

103 *About the IAPP*, INT'L ASS'N OF PRIVACY PROF'LS, https://www.privacyassociation.org/about_iapp (last visited June 2, 2013).

104 *IAPP Certification*, INT'L ASS'N OF PRIVACY PROF'LS, https://www.privacyassociation.org/certification (last visited June 2, 2013).

105 *See* Deanne Katz, *7 Hot Practice Areas to Grow Your Law Practice*, FIND LAW STRATEGIST BLOG (Sept. 12, 2012, 5:47 AM), http://blogs.findlaw.com/strategist/2012/09/7-hot-practice-areas-to-grow-your-law-practice.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+FL Strategist+(Strategist) (citing privacy law as a fast growing field within the legal profession); *The New "Hot" In-House Practice Area: Privacy Law*, INHOUSE INSIDER (Sept. 10, 2012), http://www.inhouseinsider.com/the-new-hot-in-house-practice-area-privacy-law/ (discussing the trend of companies hiring in-house counsel for assistance with privacy law issues).

privacy practices and relevant privacy law.[106] Privacy seal and certification programs have also been created,[107] and several self-regulatory organizations provide oversight and enforcement of voluntarily adopted privacy policies, advice, and support to businesses on privacy issues; handle consumer complaints; and monitor members' privacy commitments.[108] In contrast to Smith's observations in 1994, companies now promote privacy leadership and expend resources to meet privacy goals.[109]

Similar cracks have appeared in the account of comprehensive and successful attention to privacy by corporations under the mandate of E.U. privacy laws. A recently released multidisciplinary report reviewing the European Union's Data Protection Directive, for example, found that a focus on specific mandated process "risks creating an organisational culture that focuses on meeting formalities to create paper regulatory compliance (via check boxes, policies, notifications, contracts . . .), rather than promoting effective good data protection practices."[110] One commentator noted that "[t]he privacy advocacy community has generally not made extensive use of the complaints investigation and resolution process under data protection law."[111] He continued, "[i]t is indeed striking how few complaints have been lodged by European advocacy groups under their stronger and more comprehensive data protection laws" despite the fact that doing so "cost[s] no money and very little time."[112] This paradox is attributed to the fact that data protection agencies are relatively "under-resourced" and legally "constrained," and that some "do not have enforcement powers"[113] or simply have not used them.[114]

106 *See, e.g.*, PRICEWATERHOUSECOOPERS, FORTIFYING YOUR DEFENSES: THE ROLE OF INTERNAL AUDIT IN ASSURING DATA SECURITY AND PRIVACY (2012).

107 For example, TRUSTe, an online privacy seal program, was founded in 1997 and currently has seals at more than 5000 websites. *See TRUSTe Press and News*, TRUSTE, http://www.truste.com/about_TRUSTe/press-room.html (last visited June 28, 2013).

108 *See id.* The Better Business Bureau launched a privacy seal program shortly thereafter and its Children's Advertising Review Unit is the primary self-regulatory program for web sites directed at children. *See* CHILDREN'S ADVER. REVIEW UNIT, SELF-REGULATORY PROGRAM FOR CHILDREN'S ADVERTISING 3 (9th ed. 2009).

109 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 251.

110 ROBINSON ET AL., *supra* note 3, at 39.

111 COLIN J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE 118 (2008).

112 *Id.* at 122.

113 *Id.* at 118; *see also* Determann, *supra* note **Error! Bookmark not defined.**, at ¶ 9 (discussing Europe's historic failure to enforce data protection laws).

114 *See* Determann, *supra* note **Error! Bookmark not defined.**, at ¶ 8. (citing Ruth Hill Bro, *Life in the Fast Lane: Government Enforcement and the Risks of Privacy*

Accordingly, as one comparative scholar recently summarized, "there is still a wide gap between assertions by European data protection authorities and legal commentaries as to what is allowed and forbidden and what companies and government authorities are actually doing and getting away with."[115] These shortcomings are particularly acute with regards to regulatory adaptivity to new technological contexts. Privacy protection in the social media context, for example, is limited by the E.U. Directive's limited coverage of data processing by individuals for personal and private household purposes and a few provisions that might govern data breach notifications and "data collection through cookies and other tracking technologies."[116]

Perhaps most basically, by focusing on the abstract regulatory framework rather than its granular implementation, narratives regarding European regulation gloss over significant distinctions in approaches to the governance of privacy adopted by different E.U. member states. Each has its own distinct history of privacy regulation, agency models, approaches to enforcement, penalty structures, and even formal rules.

The Privacy Directive—like all E.U. Directives—was addressed to member states, but it is not legally binding on citizens until implemented in national laws.[117] Thus, although privacy regulation in each E.U. member nation complies with the general floor set by the governing framework and nations often adopt isomorphic regulatory institutions, they diverge in important detail regarding specific instruments available to regulators.[118] This in turn has led to the evolution of different means of exercising enforcement authority and different definitions of privacy in light of each nation's political culture and social context.[119] A consideration of privacy reforms informed by actual successes and failures, therefore, must take account of multiple European privacy landscapes, and the vast differences in practice that they have provoked.

II. INVESTIGATING PRIVACY "ON THE GROUND"

To that end, we have embarked on a wide-ranging project to collect

---

Noncompliance, 6 PRIVACY & SEC. L. REP. (BNA) 32 (2007) ("[C]ontaining reports on the first significant enforcement actions in Europe, which did not materialize until the mid-2000s, over 30 years after the first data protection laws were enacted in Europe.")).

115 *Id.* at ¶ 9.

116 *Id.* at ¶¶ 10–11.

117 *See* Bignami, *Transgovernmental Networks*, *supra* note 25, at 819 (explaining that the directive requires EU members to enact laws to implement the directive's provisions).

118 *See* NEWMAN, *supra* note 25, at 32–33, 94, 125–27

119 *See id.*; *infra* notes 246, 318–320, 336and accompanying text.

qualitative and quantitative empirical information documenting privacy's operationalization "on the ground" across a number of jurisdictions in North America and Europe. Central to this effort has been the execution of semi-structured qualitative interviews with privacy "leads"—those corporate managers or officers in charge of the privacy function within their firms—as well as wider ranging interviews with local privacy regulators and independent lawyers and privacy professionals involved with jurisdiction-specific compliance.[120] Additional research involved the review of internal organizational charts, process documentation, and discussions with managers and engineers responsible for policy implementation in the firms whose privacy leads we interviewed more formally.

The privacy leads interviewed, referred to in this Article as "Chief Privacy Officers" ("CPOs") or "Data Privacy Officers" ("DPOs"), included those identified as field leaders by domain experts—leading privacy thinkers (both lawyers and nonlawyers) drawn from academia, legal practice (in-house and firms), trade groups, advocacy groups, and consultancies, regulators, and journalists focusing on privacy issues.

Our process of identification was intended to pinpoint those leaders and firms to whom others in the field look when ascertaining best practices. It was not intended to elicit responses generalizable to firms broadly. This methodology offered a window into something more specific: a granular insight into the elements and approaches taken by those who others in the field identify as leaders, and thus the practices that provide legitimacy in the privacy domain. The selection method sought to uncover indications of developments in the privacy field more generally. Snowball samples tend to identify participants with thick social networks in a field; the interviews accordingly sought to capture the way in which "key informants" at the center of the privacy field reflect the broader privacy discourse of which they are a part. Similarly, because our respondents' corporations are likely

---

[120] The research has involved over sixty interviews in North America and Europe. Initial interviews, running an hour-and-a-half to two-and-a-quarter hours, were conducted primarily in person between 2008 and 2012; European interviews occurred from 2010 to 2012. Two of the U.S. interviews were conducted by phone but were otherwise identical. Interviews took place in conference rooms at the offices of the interviewees or at off-site locations at the preference of the interviewees. 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, to collect additional information about corporate practices and procedures, and confirm the continued validity of the data. The policy and practice materials—including employee training materials—were shared both in person and remotely, by access to intranet resources, and over the internet. The transcripts from all interviews conducted are on file with the authors.

to be more sensitive to shifts in regulatory structures and other external forces shaping the "social license" under which they operate, they may provide fruitful indicators of important changes in regulatory and market forces.[121]

We do not present our interviewees' reflections on the way the privacy discourse is framed in isolation, but in conjunction with a descriptive, historical, and documentary account of the development of the privacy field in which CPOs and corporations are only one set of players. The privacy leaders interviewed were very diverse in terms of personal background and type of firm in which they worked,[122] but most of those identified work at large corporations—the size company that research suggests has a greater vested interest in establishing a positive reputation for compliance with regulators[123] and maintaining legitimacy with other external constituencies.[124] With the exception of size, the privacy professionals interviewed were heterogeneous. Some are lawyers; others have operational or technical expertise. A number have worked in government, while most have had exclusively private-sector careers. They also vary in terms of the substantive authority of those to whom they report.

Despite this diversity, the interviewees within each jurisdiction conveyed a high degree of coherence regarding the constellation of issues about which we asked—namely, how corporations define privacy and operationalize its protection, as well as the extra- and intra-firm forces that shape those understandings. Specifically, they presented important consistency by nationality as to: a legal "compliance" approach's relevance to corporate privacy practices; the way in which privacy concerns are

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

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

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

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

framed within corporations, and the architectures implemented to address those concerns; and the role of a variety of external forces and internal corporate factors—in particular formal legal mandates, regulator behavior, professions, and various constituencies inside and outside the firm—in shaping that frame. In each jurisdiction, these interviews offer a window into both extant and emerging corporate privacy practices in corporations recognized as leaders, and into the elements of the operative privacy field that shape those practices.

III. FINDINGS ON PRIVACY "ON THE GROUND" IN THE UNITED STATES

The previous two articles documenting research in the United States offer a model for examining privacy on the ground. In particular, they provide data as to three aspects of the U.S. privacy landscape: (1) corporate understandings of privacy within leading U.S. firms; (2) an emerging set of resulting corporate privacy practices and architectures; and (3) insight regarding the particular elements of the U.S. privacy field—legal and non-legal—that coalesce to shape these behaviors.[125] Accordingly, they offer the basis for a new account of U.S. privacy governance, including the relevant factors that combine to catalyze particular privacy behaviors and the capacity for adaptation by regulators and regulated parties in the face of new privacy challenges.[126]

A. Emerging U.S. Privacy Understandings

Our U.S. interviewees were strikingly uniform in their descriptions of the framework through which they approached privacy and the management structures they created to support their work.[127] Although interviewees mentioned specific privacy laws, they explained that such provisions played a limited role in shaping their understanding of what corporations must do to protect privacy.[128] As one interviewee explained, "the law in privacy will only get you so far."[129] Another indicated that in many areas there is simply no law on the books.[130] Existing laws thus establish a minimum level of privacy protection, and officers must "build

125 *See generally* Bamberger & Mulligan, *New Governance*, *supra* note 12; Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6.

126 *See* Bamberger & Mulligan, *New Governance*, *supra* note 12, at 480; Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 260–63.

127 Bamberger & Mulligan, *New Governance*, *supra* note 12, at 486.

128 *Id.*

129 *Id.*

130 *Id.*

from there."[131]

In particular, our respondents emphasized that specific procedural rules informed by a commitment to principles of "informational self-determination" are irrelevant to many decisions that companies must make.[132] Specifically, such rules fail to guide companies in navigating new areas of privacy concern.[133] New products and services may derive their value from information sharing between companies and consumers.[134] Companies may be unclear on whether they can reuse and repurpose consumer information.[135] In some cases, they may be able to manipulate and profit from data supplied by consumers without violating the letter of the law.[136] Traditional privacy debates about security and access, and notice and consent, provide insufficient guidance in these emerging contexts.[137]

One example of this phenomenon arises in the context of "ubiquitous computing."[138] When companies use ubiquitous computing, data is constantly used and transferred.[139] These transfers themselves may constitute private data, as they may indicate that the user holds a certain account, uses certain products or services, or needs specific medical treatment.[140] They may even reveal the location of the user.[141] In each of these examples, the user may have been aware of the company's privacy practices and the company may have complied with applicable law, but such transactions raise additional privacy concerns.[142]

Although the U.S. interviewees reported a "reactive" approach to privacy laws, they also described significant changes in how corporations have approached privacy since Smith's 1994 study.[143] They explained,

131 *Id.*

132 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 266.

133 *Id.*

134 *Id.*

135 *Id.*

136 *Id.* at 266–67.

137 *Id.*

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

139 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 267.

140 *Id.*

141 *Id.*

142 *See id*.

143 *Id.* at 269.

fairly uniformly, that the corporations are approaching privacy issues in a variety of contexts with an eye toward understanding and meeting consumer expectations in addition to assuring legal compliance.[144] As technology and business have evolved, so have consumer expectations.[145] Corporations, faced with legal rules that fall short of protecting privacy-related consumer expectations or guiding corporations as to how to do so, have adopted policies and approaches to identify and protect them in the face of rapid technological innovation.[146] They have also responded by integrating privacy practices into general corporate decisionmaking.[147] This risk-management approach stands in contrast to the informational self-determination that underlies much of traditional privacy law.[148]

Interviewees emphasized the importance of internal "company law," which helps provide consistent privacy protection throughout the firm, even where the firm's business spans multiple jurisdictions with different regulations.[149] Such internal "law" addresses not only legal requirements but also policy preferences.[150] Companies seek to adopt internal rules "consistent with [their] global corporate values, and consistent with evolving customer expectations."[151] Every respondent included this notion of consumer expectations, in some form, in describing their company's conception of privacy.[152] They used normative words such as "integrity" and "responsibility" to describe this approach, concluding that privacy "equates to trust."[153]

This consumer-based framework affects how firms manage privacy.[154] Companies look to not only the current privacy climate but also what lies ahead, knowing that technology, business models, and expectations are constantly in flux.[155] Furthermore, they no longer approach privacy with a predominantly compliance-based strategy.[156] Instead, firms focus on risk management, attempting to prevent breaching consumer expectations while

144 *Id.*
145 *Id.*
146 *Id.*
147 *Id.*
148 *Id.*
149 *Id.*
150 *Id.* at 270.
151 *Id.*
152 *Id.*
153 *Id.*
154 *Id.* at 271.
155 *Id.*
156 *Id.* at 272.

maximizing business goals.[157] Privacy in the United States has thus become a forward-looking process in which firms rely in large part on internal firm policies centered on consumer expectations to guide privacy decisions rather than exclusively on laws and regulations.[158]

1. Emerging Corporate Best Practices: Operationalizing Privacy Within the Firm

Our interviewees described two important trends in the architecture of internal corporate privacy management that they understood to be integral to this risk-management function. First, companies need a powerful and relatively autonomous professional privacy officer at the top level of management, whose job includes substantial engagement with external stakeholders.[159] Second, firms require architectures intended to distribute privacy decisionmaking throughout firm units. This is most notably achieved by: (a) including privacy in existing risk management processes and (b) embedding privacy decisionmaking 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.[160]

2. The Chief Privacy Officer

The first identified trend involves the construction of the CPO function, itself nonexistent a decade ago, and the effect of this new type of officer on corporate decisionmaking.[161] The increasing power of corporate privacy leaders within the corporate structure is critical to this development. The privacy officers interviewed were part of senior management, often within the "C-suite."[162] This enables CPOs to promote privacy policies from the top down and in front of corporate boards.[163] Furthermore, at this level, CPOs are involved in strategic, high-level decisions.[164] They can integrate privacy concerns into the general

157 *See id.*
158 *See id.* at 269-72.
159 *See* Bamberger & Mulligan, *New Governance*, *supra* note 12, at 479–80.
160 *See id.*at 479–80, 495.
161 *Id.* at 479.
162 *Id.*
163 *Id.*
164 *Id.*

corporate decisionmaking process.[165]

Interviewees also explained that the ambiguity in American privacy law leads firms to rely heavily on the expertise of CPOs.[166] This in turn helps increase CPOs' autonomy and authority.[167] The dynamic, risk-oriented nature of privacy obscures clear solutions for top managers because "the rules change," because "[c]ustomer expectation changes."[168] This results in a deep professional deference to CPOs, and gives them broad discretion to shape their organizations' privacy agendas.[169] As one CPO explained, "[T]ypically, 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."[170] This further underscores the external orientation of the high-level privacy officers interviewed. To meet the demands of an ever-changing privacy landscape resulting from new societal values, technology, and business models, CPOs spend approximately half of their time working with external actors, including the government, advocates, and other privacy officers.[171] This is necessary, they explain, to keep firm policies in line with evolving privacy norms.[172] Both the CPO's professional autonomy and his or her role as a translator of external norms within the firm are consistent with organizational research demonstrating the importance of professionals who interpret and mediate uncertain external environments for the firm,[173] and exploring the ways in which individuals who shape and control external resources—like legal legitimacy—become increasingly powerful firm decision makers.[174]

3. *Operationalizing Privacy*

This process of translating external norms—"operationalization"—is reflected in two key ways across and downward in leading U.S. firms:

---

165 *Id.*

166 *Id.*

167 *Id.*

168 *Id.* at 490.

169 *Id.* at 489–90.

170 *Id.* at 490.

171 *Id.* at 479.

172 *Id.*

173 *See* Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 AM. ECON. REV. 941, 946 (1963) (explaining that professionals like doctors sell information to those faced with risk and uncertainty).

174 *See* JEFFREY PFEFFER & GERALD R. SALANCIK, THE EXTERNAL CONTROL OF ORGANIZATIONS: A RESOURCE DEPENDENCE PERSPECTIVE xiii (1978).

(1) by integrating privacy into existing risk management functions as a means of aligning privacy with other core firm goals[175] and (2) by distributing expertise and accountability throughout firm decisionmaking.[176]

First, those we interviewed emphasized that by articulating privacy in U.S. firms as a risk-management function, privacy can be included in enterprise-wide governance activities, including enterprise risk management and audit.[177] This is significant for a number of reasons. Most generally, it provides a means for adding privacy to the list of issues considered in setting the overall policy and strategic direction of the firm.[178] Additionally, such integration makes greater resources available to each issue through economies of scale. Integrating privacy within a single "fundamental governance model" establishes a "compliance process, an oversight process, [and] . . . a risk-management [process]" that is applied to all management issues.[179] By combining these processes, firms can reduce their overhead.[180]

Privacy red flags, for example, can be included in the technology system that tracks a company's products or processes.[181] This is generally the same system used to flag problems with production, cost, and performance.[182] Such integration, moreover, offers business lines a "deep understanding of what that data is that goes on the systems" within a firm, and permits privacy officers to profit from system-wide audit activities, including those reported to the board.[183]

Using audits and risk management was particularly important to the interviewees because it supported the integration of privacy, as it required distributed expertise to accompany the responsibility that was placed upon business units. All of the CPOs interviewed agreed that a distributed network of employees within each business unit, trained in the practices and tools of information privacy, is key to addressing privacy issues upfront during project development and execution.[184]

This process of operationalizing privacy begins with the collaborative

175 Bamberger & Mulligan, *New Governance, supra* note 12, at 479.
176 *Id.*
177 *Id.*
178 *Id.*
179 *Id.* at 493.
180 *Id.*
181 *Id.*
182 *Id.*
183 *Id.* at 494.
184 *Id.* at 494–95.

development of policies and practices regarding the treatment of personal information, including both subject-specific experts under the CPO's direct authority and business-line executives responsible for the domain that those guidelines will govern.[185] The privacy leaders 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," describing, "a cross-functional team that had representation from all of the lines of business."[186] Engaging business units in developing privacy policy enhances CPOs' ability to hold executives in those units accountable for implementing such policies.[187] As one CPO 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 . . . '[g]o audit these people.'"[188] The CPOs found that holding executives responsible for privacy is essential to overall firm privacy buy-in and management.[189]

Beyond the inclusion of business units in setting policy, CPOs also reported using "embedded" employees to distribute the responsibility of privacy compliance.[190] These employees are specially trained and are afforded "a mix of privacy decisional tools, technical decision-guidance mechanisms, and business-unit appropriate training."[191] These employees give CPOs reach across the company and deeper knowledge of business activity. For example, one CPO reported that his organization employed twenty people dedicated solely to privacy, and also directed 300 more to implement privacy through their business units.[192]

The firms differed in how they structured such embedment. Some had very centralized structure, assigning each business unit specific privacy leads that would report to the CPO.[193] The leads were directly involved in decisions of the business unit and helped design new products and services.[194] Other firms had full-time privacy employees who specialized

[185] *Id.* at 495.

[186] *Id.*

[187] *Id.*

[188] *Id.*

[189] *Id.*

[190] *Id.* at 496.

[191] *Id.*

[192] *Id.* Another CPO said his firm had thirty to forty fulltime employees, and 400 part-time privacy workers. A third reported about eighteen full-time privacy managers, not including lawyers, who focused on separate business units within the firm. *Id.*

[193] *Id.*

[194] *Id.*

in particular subject areas.[195] Others employed an overlay of privacy experts assigned to countries, geographic regions, or groups of countries.[196] These subject-matter experts generally reported directly to executives within the firm other than the CPO.[197] In still other instances, firms assigned a "lead" privacy expert, who reported to the CPO, but also assigned employees within business units to manage privacy but not report directly to the CPO.[198] The embedded privacy staff engaged in a variety of activities depending on their experience.

Lower-level embedded privacy staff act as issue- spotters or triage personnel, identifying issues for consideration by others dealing more specifically with privacy.. Those higher-up the privacy ladder include full-time privacy professionals responsible for developing appropriate business-level policies through coordination with both the CPO's office and senior officers in the business unit.

In some organizations, non-experts making business-line decisions rely on workflow and design documentation and technology to provide "self-serve" privacy guidance . One firm, for example, employs a suite of self-help tools for business lines, which assist managers in passing privacy "checkpoints," and a privacy impact assessment tool that uses a dynamic set of questions to enable the reporting and auditing of compliance with both internal and external privacy requirements. Others, by contrast, use privacy documentation primarily to surface issues to be referred to experts, rather than to direct their resolution.[199]

Whatever the structure, the CPOs uniformly viewed embedded employees as crucial to implementing privacy for several reasons. By training existing staff, firms can reduce privacy risks through regular business management, rather than as a separate regulatory-driven matter.[200] Thus, integrating responsibility and expertise throughout the firm allows for the organic consideration of privacy requirements.[201] This increases overall privacy management; as one CPO explained, it is 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."[202]

---

195 *Id.*

196 *Id.*

197 *Id.* at 497.

198 *Id.*

199 *Id.*

200 *Id.*

201 *Id.*

202 *Id.*

B. A New U.S. Privacy Story

This new account of U.S. corporate privacy practices points to elements of the privacy landscape heretofore absent from the dominant narratives of the American privacy field. Although the research suggests important changes in corporate privacy behaviors—in terms of both understandings of privacy and the best practices they produce—such changes cannot be attributed to legal reform long sought by advocates. Privacy regulations are still scattered across specific sectors, Congress has not adopted omnibus legislation reflecting the FIPPs, and there is still no independent privacy administrator like that of the European Union.[203]

These changes suggest a new narrative of the American privacy field. This narrative reflects a field that has been positively shaped by the incomplete, and comparatively late, institutionalization of privacy governance, in that it has allowed dynamism and adaptability in the face of rapid changes in the use and treatment of personal data. Specifically, our interviews suggest that the new emphasis on consumers, markets, and a risk-management approach—and the architectures intended to reflect these approaches—emerged against the backdrop of several intertwined developments central to the creation of a network of normative inputs regarding privacy: the FTC's expanded application of its consumer-protection enforcement authority in the privacy context,[204] new state statutes mandating data breach disclosure,[205] the media's increased interest in privacy issues,[206] and the professionalization of the privacy-officer community.[207] Together, these forces and a variety of actors shaped evolving definitions of privacy and dynamic understandings of how those definitions should be reflected in privacy decisionmaking within firms.[208]

The development of the FTC over the past fifteen years as an "activist privacy regulator" is central to this account.[209] Although the FTC has long been the agency responsible for rulemaking and enforcement under several specific sectoral statutes regulating privacy, including the FCRA,[210] it did not direct its general consumer-protection authority to information privacy

---

203 *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 251.

204 *Id.* at 273.

205 *Id.* at 275.

206 *Id.* at 276–77.

207 *Id.* at 277.

208 *Id.* at 308–11.

209 *See id.* at 273–75.

210 Fair Credit Reporting Act, 15 U.S.C. §§ 1681–81x (2012). The Act governs the accuracy, integrity, and dissemination of consumer credit reports. *Id.* § 1681, 1681(b), 1681(e).

until 1995, when it first began to hold workshops "to identify the consumer protection and competition implications of the globalization and technological innovation at the core of the internet revolution."[211] Since that time, the FTC has worked with outside experts and stakeholders to develop privacy norms and outline the role of privacy in the online marketplace.[212] The FTC is now the leading domestic agency that defines and enforces privacy practices.[213]

The FTC has achieved this status by taking advantage of its broad discretion to define what falls under the "unfair and deceptive" practices standard[214] of the Federal Trade Commission Act.[215] The FTC also used a number of administrative tools to solidify its role as a privacy regulator, including publicity, research, expert opinion, best-practices guidance, Federal Advisory Committees, support of certification programs, and a participatory process that stimulated dialogue between advocates, industry representatives, and academics.[216] Furthermore, the FTC negotiated with industry to develop self-enforced codes of conduct.[217] Finally, the agency swept websites to analyze their information privacy practices and encouraged owners to reassess their own practices and self-regulate.[218]

The FTC's efforts resulted in a detailed public record about the privacy implications of technologies and emerging business practices and how they relate to consumers' expectations.[219] This record, combined with the enactment by forty-five state legislatures of laws requiring disclosure to affected parties of any private information security breaches, has significantly increased transparency in corporate privacy practices.[220] This transparency in turn opened up private companies to regulation, negative press, and vigorous public scrutiny and debate about their practices and obligations.[221] The FTC's participatory fora proved to be an ideal venue for these debates. FTC workshops gave advocates a sustained platform for expressing privacy concerns to an able regulator as well as the press, congressional staff, trade associations, lobbyists, and industry executives.

211 Bamberger & Mulligan, *New Governance*, *supra* note 12, at 484.
212 *Id.*
213 *Id.*
214 *Id.*
215 Federal Trade Commission Act, 15 U.S.C. § 45 (2012).
216 Bamberger & Mulligan, *New Governance*, *supra* note 12, at 484.
217 *Id.*
218 *Id.*
219 *Id.*
220 *Id.*
221 *Id.*

Through this dialogue, they were able to both expose and shape corporate privacy practices.[222]

These concurrent developments brought business uses of consumer information under increased scrutiny, and, importantly, re-oriented the inquiry around questions of fairness and alignment with consumers' expectations. This evolving understanding of privacy contrasts starkly with the static procedural requirements mandated by sectoral privacy statutes.[223] Furthermore, it reflects the normative idea that privacy should protect consumers and meet their expectations about the use of their personal information, even where firms attempt to use procedural formalities to create tremendous leeway.[224]

This consumer-oriented notion of privacy protection alters the impact of enforcement in two ways. First, the FTC is increasingly using its enforcement powers to identify, target, and publicize privacy practices that it deems "unfair and deceptive," even where those practices include some amount of disclosure to consumers.[225] Second, the FTC accepts, and responds to, complaints from advocacy organizations requesting that the agency investigate corporate privacy practices, thus allowing advocates to harness the formidable power and resources of the agency.[226] These new enforcement measures have increased uncertainty among firms about how to satisfy privacy requirements.[227] Firms are thus forced to focus not just on complying with existing law and perfecting legal disclaimers, but on understanding and meeting privacy norms as they relate to new products and services.[228]

The FTC is thus located at the center of a loose framework of actors and institutions that has fostered a shift in corporate approaches to privacy, moving away from legal formalism and toward the treatment of privacy as an issue of managing risk against a backdrop of consumer expectations.[229] It "provides an 'extra layer' that . . . [no] 'privacy officer wants to skirt with . . . . You have to analyze . . . [things] in terms of the strict compliance line versus what can we do above and beyond that that's appropriate.'"[230] Modern privacy practices must reflect both the letter of the law and the

222 *Id.* at 485.
223 *Id.*
224 *Id.*
225 *Id.*
226 *Id.*
227 *Id.*
228 *Id.*
229 *Id.* at 487.
230 *Id.*

evolving best practices set out in the FTC guidelines, staff reports, investigations, and enforcement actions.

State data breach notification laws contributed to the reconceptualization of privacy as a risk management activity[231] as they transformed previously unnoticeable corporate lapses into press events. The ensuing cycle of highly reported breaches, investigations, and settlements establishing mandatory practices for breaching entities, combined with the FTC actions, have resulted in the public availability of information about privacy risks and best practices. Such transparency has further been exploited by privacy advocates, keeping privacy and data protection on the front burner and demanding attention all the way up to the level of the board.[232]

Finally, the CPOs interviewed all emphasized the importance of the growing professional privacy community in helping firms navigate the ambiguities of the consumer-expectation-oriented privacy framework.[233] They described professional associations, including the IAPP, as particularly useful sources of guidance and strategic advice.[234] The IAPP publishes information on best practices and gives privacy professionals an opportunity to network and share information and guidance.[235] This information sharing saves costs by pooling valuable knowledge and helping CPOs advocate for new practices within their organizations.[236] As one CPO stated, it "is really helpful for very resource-strapped groups . . . . [I]f there's a change in privacy, it's so ill-understood outside of our little enclave that for me to say, 'I need five hundred thousand dollars to do a research project based on opt in,' it ain't happening."[237] CPOs fill this knowledge gap with information shared by leading companies: "So, with other corporate leaders, you know, the Microsofts and the Axioms and the P&Gs and others who really have phenomenal programs, there's a lot of . . . sharing that goes on."[238] One interviewee attributed this willingness to share information to the fact that protection of private information is more valuable to an industry as a whole than to any individual company.[239]

---

231 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 275–76.

232 *See, e.g.*, *Chronology of Data Breaches: Security Breaches 2005–Present*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach (last updated June 2, 2013).

233 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 277.

234 *Id.*

235 *Id.* at 277–78.

236 *Id.* at 278.

237 *Id.*

238 *Id.*

239 *Id.*

This lack of competition over privacy has fostered widespread information sharing and has supported the institutionalization of similar practices across sectors and firms.[240]

IV. RESEARCH ON EUROPEAN PRIVACY "ON THE GROUND"

A. Privacy on the Ground in Germany

Our work in Germany provides a nuanced picture of how the rich mix of regulatory institutions and privacy professionals combine with other aspects of the regulatory and corporate culture to manage privacy. This work generated our most surprising, and perhaps even counter-intuitive, finding: the small tier of German privacy "leaders" reflected practices remarkably akin to those we documented in leading U.S. firms.

Our interviews with those top German leaders and our survey of responsibilities and practices reveal numerous similarities to the management approaches toward privacy documented in the United States. This is somewhat startling given the vast and obvious differences in regulatory substance and structure between the two countries. In global debates, Germany's legal commitment to privacy protection is held up as representing one end of the spectrum, while the United States is placed at the other end.[241] It is also remarkable given that the definitions of privacy at work within the two countries' firms are similarly distinct. In the United States, privacy has a decidedly amorphous definition at its edge. Though encompassing some adherence to data protection principles reflected in the E.U. Data Protection Directive and other instruments, privacy in the United States is infused by key regulators' consumer protection oriented objectives in a manner that makes achieving privacy obligations a more forward-

240 *Id.*

241 A case involving Wikipedia in Germany and the United States illustrates the spectrum. In 1990, two people killed an actor and were sent to prison. Spiros Simitis, *Privacy—An Endless Debate?*, 98 CAL. L. REV. 1989, 1994 (2010). When they were released in 2007 and 2008, they sued to have their names removed from prior publications and to prohibit any further published reference to their crime. *Id.* Their lawyer argued that they should be given an opportunity to rehabilitate and "lead their life without being publicly stigmatized." *Id.* Wikipedia's German-language version thus deleted all mention of the two men in its article about the murder victim. *Id.* However, similar efforts in the United States have stalled and are unlikely to be successful. *Id.* Similarly, "Google's rollout of its Street View service in North America in 2007 provoked little concern about the privacy implications of private homes and individuals being easily viewed by potentially millions of persons." Roger C. Geissler, *Private Eyes Watching You: Google Street View and the Right to an Inviolate Personality*, 63 HASTINGS L.J. 897, 897 (2012). "In contrast, Street View's reception in Europe, particularly in Germany, has been marked by episodes of both public outrage and government concern." *Id.*

looking and dynamic task.[242] In Germany, privacy efforts center around compliance with data protection law, as they do in Spain and France.[243] However, in Germany, data protection is more solidly and specifically influenced by other ethical frameworks that, as with consumer protection in the U.S. context, require data protection officers (DPOs)—the European equivalent of CPOs—to more actively engage in sorting out privacy's meaning with divergent members of the privacy field. Specifically, the link between the atrocities committed during World War II and the enabling role personal data collections played in carrying them out have firmly nested privacy in a broader ethical framework of human dignity.[244] Furthermore, the strong position of workers' interests within the Germany economy—including representation within firms and their boards—coupled with ongoing workplace privacy issues creates a second ethical framework that infuses fairness and respect for employees as well as customers into data protection work.[245] These broader ethical frameworks facilitate support for DPOs from additional institutional structures—the work councils and board representatives—and create a richer language that DPOs leverage to engage the firm leadership and move beyond a compliance mentality.[246]

As it has in the United States, the less fixed and regulator-defined definition of privacy at work in German firms has empowered the DPOs.[247] What is perhaps most interesting about the role of the DPOs, however, is the recent accretion of power, authority, and resources, despite an unchanged statutory framework requiring DPO positions in German firms.[248] Our interviews suggest that the statutory command was sufficient in many—though certainly far from all—instances to establish a data protection office with some clout; however, it took risks to firm reputation caused by increased publicity, penalties, and data breaches to fully realize the DPO roles they now occupy.[249] Given the disparate legal frameworks and divergent definitions of privacy at work in German and U.S. firms,[250] we were struck by the extent of similarity among their internal structures and practices. On nearly every metric we identified as significant and

[242] *See supra* notes 155–162 and accompanying text.
[243] *See infra* Parts IV.B, C.
[244] *See infra* note 264 and accompanying text.
[245] *See infra* Part IV.A.1.
[246] *See infra* Part IV.A.1.
[247] *See infra* Part IV.A.2.a.
[248] *See infra* Part IV.A.2.a.
[249] *See infra* Part IV.A.2.a,
[250] *See infra* Part IV.A.1.

shared across our U.S. cohort, German firms presented similar institutional choices. From the position of the CPO or DPO within the firm[251] and decisions about personnel[252] to relationships with the board and regulators,[253] the U.S. and German approaches were similar. The German firms generally displayed slightly fuller expressions of the traits we identified in our analysis of U.S. firms as considered to be excelling on privacy management.[254]

DPOs are strategic players within German businesses, as is reflected in the mix of internal and external activities they reported as well as the structures they have put in place to embed privacy throughout firms.[255] Despite overwhelmingly similar efforts to embed privacy within the firm, German DPOs interviewed presented diverging views about whether their efforts ought to be centralized or decentralized.[256] This is distinct from the United States, where all the CPOs sought to create a distributed and embedded privacy staff with indirect reporting structures throughout the firm.[257] Some DPOs followed a similar model with a similar rationale finding this to be the most efficient and effective way to address privacy during the early phases of projects. Others felt that the statutory framework under which they operated requires a more centralized and advisory role, despite acknowledging potential limitations to this more arms-length arrangement. However, even those firms pursuing a more decentralized approach have extensive embedded privacy staff.

As with our U.S. cohort,[258] the privacy leaders interviewed come from firms that are heterogeneous on every metric except size. Most have a global presence, although the extent of their international operations varies; some are highly diversified, others have a single core business; and most of our interviewees come from data intensive businesses.

1. Privacy's Meaning: Data Protection Nested in Broader Ethical Frameworks

The definition of privacy that emerged from our conversations with DPOs reflects the heavy influence of data protection law. Within German firms, the force of data protection is strong. The "set of rules . . . the legal

[251] *See supra* note 166 and accompanying text; *infra* Part IV.A.2.a.
[252] *See supra* notes 184–196 and accompanying text; *infra* Part IV.A.2.c.
[253] *See supra* notes 169–170 and accompanying text; *infra* Part IV.A.2.a.
[254] *See infra* Part IV.A.2.a–c.
[255] *See infra* Part IV.A.2.b–c.
[256] *See infra* Part IV.A.2.c.
[257] *See supra* notes 190–192 and accompanying text.
[258] Bamberger & Muligan, *Privacy on the Books*, *supra* note 6, at 264.

regime", and "the data protection laws" were routinely cited as the "fundamental" source and "really the starting point" for defining the meaning of privacy and firms' obligations. For all interviewees, a key goal was "to try to do [the firm's work] in as compliant" a manner as possible. All firms thus strongly aligned privacy with data protection.

The meaning of privacy within the firms goes beyond legal requirements of data protection and is tied to the broader concept of privacy and the overall human rights framework, as it does in France.[259] While DPOs in both countries focused predominantly on data protection, the related concept of privacy—the right to respect for private and family life, home, and communications[260]—informs the companies' perspective on data protection obligations, particularly with respect to employees.[261] DPOs reported using the broader concept of privacy instrumentally to escape the compliance mentality associated with data protection: "I use privacy to have more room to explain different concepts. But from the content, it's driven from the requirements by law, which is basically the E.U. Directive and the relevant national laws." In our French interviews, broader human rights concepts of freedom and dignity were the dominant harmony to the melody of compliance,[262] but other ethical frameworks dominated our German interviews.

Two key frameworks inform German corporations' understanding of privacy, one borne of history, the other of the political economy. Commentators attribute Germany's fidelity to privacy rights in part to its dark history.[263] In several instances, the compliance oriented meaning of privacy was situated in broader ethical obligations on firms and the government stemming from the atrocities of World War II, in which some corporations were complicit or active participants and beneficiaries,[264] and

259 *See infra* Part IV.C.1.

260 Charter of Fundamental Rights of the European Union 364/01 art. 7, 2000 O.J. (364) 10.

261 The Charter of Fundamental Rights of the European Union 2000 differentiates between data protection and privacy. *Id.* at 7–8.

262 *See infra* Party IV.C.1.

263 For example, James Whitman notes in his exploration of European privacy conceptions versus American conceptions that "German law was peculiarly formed by the events of the Nazi period and after" and that "German privacy law [was established] . . . in connection with the painful experience of Nazism." Whitman, *supra* note 89, at 1172, 1180. In addition, the data collection practices of the DDR-Regime in East Germany may have informed the privacy protective stance of the German government. Johannes Masing, *Herausforderungen des Datenschutzes*, 2012 NEUE JURISTISCHE WOCHENSCHRIFT, 2305, 2305 (2012) (Ger.).

264 *See* S. Jonathan Wiesen, *German Industry and the Third Reich: Fifty Years of Forgetting and Remembering*, 13 DIMENSIONS: J. HOLOCAUST STUD. (1999), *available at*

during which the collection and use of individual data contributed to the ease with which atrocities were carried out.[265] During the post-World War II reconstruction, German lawmakers strengthened personal privacy rights in an effort to prevent the government from being able to single out citizens for persecution.[266] Conceivably, because Germany's experience with abuses of human dignity was extreme, its privacy laws now lie on the protective end of the spectrum relative to those of other countries. In some industries, such as healthcare, the connection between ethical behavior generally and privacy loomed especially large. As one interviewee explained:

> That comes mostly from the Nuremburg Codex of 1947 . . . that was ages before . . . someone thought about . . . privacy, but it was the same idea . . . you have to be transparent to the people, you have to explain to them which data you collect for which purpose and what will happen with the data; so more or less the same [as] you do in the privacy field . . . if we violate privacy laws, then it's very close to violat[ing] this ethical obligation to be fair . . . .

The second dominant subtheme defining the meaning of privacy within firms is that of workers' rights, which were sometimes portrayed as representing the interests of society broadly in the firms' activities. "So the issue of data protection is also very much influenced by work councils and by unions," explained one interviewee. The DPOs interviewed reported that the power of unions and their role in negotiating around issues of workplace surveillance and data processing heavily influences the understanding of privacy, and, as discussed below, its operation:

> Data protection is an issue which is very intensively treated by works councils because in Germany . . . . [w]orks council is allowed to commonly determine certain standards [of] how employee data is treated within business processes. Because . . . in Germany—it is illegal to use employee data . . . . [t]o control the work quality, the amount of work [a]nd the behaviour of the employee without the employee's consent. And consent is reached by 'collective contracts,' we call that. Tariff contracts or intercompany contracts that define how employee data may be used in such processes and for what purposes by management.

Due to this structure, another DPO added, "the issue of data protection

http://archive.adl.org/braun/dim_13_2_forgetting.asp.

[265] Damon Greer, *Privacy in the Post-Modern Era—An Unrealized Ideal?*, 12 Sedona Conf. J. 189, 189 (2011). *See also* Geissler, *supra* note 241, at 898.

[266] *See* Whitman, *supra* note 89, at 1180–81, 1189.

is also very much influenced by work councils and by unions." The DPO explained:

> [W]e are trying [so] that our employees can trust our processes, so . . . in this part we are on the same side so we can use it to bring more awareness to our employees in the handling of personal data but as well that we are saying these are our processes, these are our regulations, we have discussed it with the works council.

The interaction between privacy and labor is a product of both Germany's legal framework and the structure of its market. As one DPO noted, "it is written in the collective labor law that the works councils have to become involved whenever monitoring employee accounts [comes] into . . . play. And that involves quite a few privacy matters." There is also a strong tradition of labor involvement in workplace matters overall, reflected in the requirement for independent labor representation in the workplace and on the board.

Some German interviewees believe the nexus between privacy and workers' rights facilitates "a discussion around . . . the values of the company," which one officer specifically connected to "trust and motivation" on the employee side. The nexus also generates a broader conversation about the balance between individual rights against company interests and societal interests. One DPO told us:

> I would argue that privacy is balancing the rights of the individuals where we collect and then process data with the interest of the company to use that data, to deal with that data, be it in our own interest or because we are obliged to process that data by regulators of whatever kind.

Others connected this privacy conversation to broader questions of corporate social responsibility. One interviewee stated that "in Germany or in Europe [generally] . . . the customer wants to be sure that the company also is very . . . correct and very responsibly acting as far as . . . personal data are concerned." The concept of customer trust made a limited showing in the DPOs' responses. Some DPOs strived to redefine the foundation and aim of privacy and data protection for the firm around employee and customer trust. One interviewee spoke clearly of his company's current shifting perspective around privacy, his role in it, and globalization—a key driver—saying:

> [A] part of that process is to rearticulate and reposition the policy first and foremost as a customer value because its background tends to come from compliance and law and risk, and so on and so forth, which is important but it's not the whole story and certainly

> for the kind of business we are—heavily consumer-focused or focused on individuals and the services we deliver, connectivity, and so on and so forth—being the trusted guardian of information and privacy is a critical factor for our success.

He went on to explain that a consumer focus is, "really the aspiration and I am in discussions with my executive board sponsor about this new set of principles, which really encapsulates this point of the value of privacy, specifically talking about going beyond compliance." He explained further that "where we are today predominantly comes from a compliance background . . . we're . . . steeped in the complexities and vagaries of European data protection law." While this was beneficial, as it had given the firm "a sensitivity towards the issues," it did not provide a strong basis outside Europe. He stated:

> [W]e've expanded beyond Europe, so more of our subscribers are based outside of Europe than inside of Europe . . . . So we've kind of come from a European heritage, looking at privacy as a compliance obligation. Privacy in markets like India, it means nothing there. Compliance in what? There's no law that deals with privacy, so what does it mean? In part, re-articulation is [not meant] to actually encompass markets that don't understand the concept but to present [privacy] as being about the value to the customer and preserving that value, and enhancing and maintaining the trust that we need to be successful.

The strong regulatory structure in Germany and the E.U. creates a platform from which DPOs feel they can engage other company executives in a conversation about privacy as a value commitment as the company enters new markets, some of which have no privacy laws. As one interviewee described in the context of negotiating binding corporate rules:

> [W]hen we introduced our first BCR, binding corporate rules . . . we had discussions on what the exact scope of the binding corporate rules should be. Should we only use them to protect what we were legally [bound] to do; protect European data that gets transferred to non-European states? Should we include[] countries like Canada and Argentina who have been determined as having adequate privacy regime[s] also at that time? Or should we have a broader scope and protect all data? And I think that was the first time when we had this discussion around values, including some of the board members who were very interested in that discussion. And we have seen also on [the] board level kind of a split approach to that one. Also on board level you find

> people who will say, "well, this could harm our business because we do more than we are legally required to do" but the then CEO said, "well, how can we explain . . . [to our] employee or a customer in let's say . . . Africa why we treat him with less respect and why we treat his data less seriously just because he happens to be in Nigeria and not in Austria or in Switzerland?" I think that was the starting point, at least the first time that I realized it, where we really started to discuss[] not only [that] . . . we need to do privacy because it's prescribed by law but to focus on that kind of more and more ethical and value-oriented way.

Another DPO similarly captured the connection between ethical corporate behavior and privacy, saying:

> [I]t would be . . . unfair if we would do more . . . activities in such countries only with the argument that, "well, there's no privacy laws; there's no . . . laws so we could do whatever we like;" that would be really unethical. And so also this ethical aspect is, I think, a very important one because . . . it is also an extremely, let's say, sensible area where you have [to] always . . . find a good balance between what is good for the business and what is also important to have a good ethical standard.

The term "trust" arose infrequently in conversations about privacy's meaning. However, for firms with a global presence, the concepts of trust and ethical obligations were identified as increasingly important methods for positioning and understanding privacy in the absence of legal constraints. DPOs appeal to privacy, as opposed to the narrow construct of data protection, to check the compliance orientation that could arise as privacy butts up against profit. The rhetoric of trust and corporate values plays a similar role in instances where DPOs are seeking to encourage beyond-compliance activities in countries with few or weak privacy laws.

While legality is the overriding definition and objective of privacy within German firms, the language of privacy is laced with references to other ethical and social constraints born of specific German experiences such as the Holocaust, the representation of and respect for workers and their interests in firm decisionmaking, and the general European connection between data protection and human rights and its implications at a time of globalization.

2. Emerging Corporate Best Practices: Operationalizing Privacy Within the German Firm

Despite the divergent legal frameworks and definitions of privacy used in the two countries, the internal structures were very similar between the U.S. and German firms we observed. The one exception was the use of decentralized and embedded privacy personnel, where some German companies parted ways from the U.S. model,[267] choosing to rely on centralized privacy experts. However, those German companies pursuing a more decentralized approach to privacy did have extensive embedded privacy staff. Below we discuss the role of the DPO, which, as with CPOs in the United States,[268] we found to be high-level, strategic, and forward-looking. This part then describes the operationalization of privacy, which, as in leading U.S. firms,[269] was achieved through the distribution of privacy expertise and accountability throughout the firm, and the integration of privacy into existing risk management functions.

a. The Data Protection Officer

As in the French regulatory context discussed below,[270] Germany had a well-developed set of rules, institutions, and practices in place that influenced the transposition of the Directive.[271] The institutions and data protection practices reflect Germany's belief in individuals' and industry's capacity to act appropriately and to identify and conform their behavior to the law.[272] From its inception, the German system has placed much responsibility for privacy within the firm.[273] The principle of corporate self-monitoring is evidenced in the overall structure of German data protection—which scholars refer to as an "advisory model,"[274] in contrast to the licensing and bureaucratically-centered model of France[275]—and in specific legal requirements such as the mandatory appointment of an internal privacy official, or *datenschutzbeauftragter*.[276] Corporate self-

---

267 *See supra* note 190 and accompanying text.

268 *See supra* notes 162–172 and accompanying text.

269 *See supra* notes 175–180 and accompanying text.

270 *See* Francesca Bignami, *Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy*, 59 AM. J. COMP. L. 411, 424–26 (2011) [hereinafter Bignami, *Cooperative Legalism*].

271 *See id.* at 426–30.

272 *See* FLAHERTY, *supra* note 10, at 25 (discussing the influence of the combination of "exacting legalism" and trust in civil servants on the structure of data protection); Bignami, *Cooperative Legalism*, *supra* note 275, at 427(discussing importance of concepts of "self-responsibility and self-control" in shaping of German data protection field).

273 Bignami, *Cooperative Legalism*, *supra* note 270, at 427.

274 *See* FLAHERTY, *supra* note 10, at 22.

275 *See* Bignami, *Cooperative Legalism*, *supra* note 270, at 424–25.

276 *See* Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Jan. 14, 2003, RGBl at § 4f(1) (Ger.). Any company that uses automated means to process personal data must appoint an internal data protection officer within one month of beginning such

monitoring is reflected in common practice as well. Trade associations play an important role in sorting out the regulatory requirements facing an industry: collaborating to produce rules, contractual clauses, and approaches and then negotiating and refining them with regulators.[277] The privacy field in Germany thus has strong statutory law and resources supporting its public administration, along with a rich and active tradition of industry participation in the formation and oversight of more detailed provisions.

A clear expression of the importance of self-governance in the German regulatory scheme is the position of the DPO. Companies that employ more than nine employees to automatically process personal data must appoint a DPO, as must companies that employ twenty or more people who process data manually, and those that process especially sensitive data or use complex systems.[278] The legal framework defines the DPOs' core competencies[279] and duties[280] to be performed, and establishes the

processing. *Id.* The obligation to appoint an internal privacy officer also applies to companies that employ twenty or more people who work with nonautomated data processing, and to companies that process especially sensitive data or use complex systems. *Id.* The definition of employee is broad including consultants, freelancers, etc. *See* GOLA ET AL., BDSG: BUNDESDATENSCHUTZGESETZ: KOMMENTAR § 3 (11th ed. 2012). The definition of employees who work with automated data is similarly broad. See *New Requirements for Data Protection Officers in Germany*, MAYER BROWN (June 8, 2011) http://www.mayerbrown.com/publications/detail.aspx?publication=1315 ("[R]egulators take a broad view when defining the categories of employees to which the [Act] applies. To a large extent, the definition encompasses every employee who works with a computer to compile, process or use personal data.") In some cases, a company will appoint an external privacy officer; the *Duesseldorfer Kreis* recommends that such an officer be employed under at least a four-year contract in order to guarantee independence and objectivity. Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 24./25. November 2010), *available at* https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Mindestanforderungen_an_Datenschutzbeauftragte/Mindestanforderungen_an_DSB_nach_4f_II_und_III_BDSG.pdf.

277 *See* Bignami, *Cooperative Legalism*, *supra* note 270, at 427. The German Association for Data Protection and Data Security (GDD)was founded in 1976 and interacts with government officials, data protection authorities, associations, and privacy experts world-wide to "strengthen effective self-regulation and corporate self-monitoring in the framework of German data protection law in order to make state supervision and controls unnecessary as far as possible." GERMAN ASSOC. FOR DATA PROTECTION AND DATA SEC., https://www.gdd.de/international/english (last visited June 6, 2013); *Promoting Self-Regulation*, GERMAN ASSOC. FOR DATA PROTECTION AND DATA SEC., https://www.gdd.de/international/english/main-tasks (last visited June 6, 2013).

278 *See supra* note 276

279 The data protection officer must be reliable and possess relevant knowledge of privacy in the legal, organizational, and technical domains. BDSG § 4f(2).

280 The duties of the DPO include identifying deficits in data protection compliance,

relationship between the DPO, the firm, and the regulator.[281] DPOs are tasked with monitoring company projects that involve the processing of personal data with the aim of fulfilling the provisions of federal and state data protection laws.[282] To ensure an officer's independence, the Act requires that the officer report directly to the company's management.[283] The company must fund continuing training for the officer and not discriminate against him or her.[284] The officer must have access to all relevant documents and data-processing locations, and be included in data-related projects and decisions.[285] The officer must be intimately familiar with Germany's privacy laws, including the constitutional rights of data subjects and employees, the applicable provisions of the Federal Data Protection Act, and the core principles of data protection in Germany.[286] The officer must also understand data security technology, risk management, and organizational management.[287] Companies may be fined €50,000 for failing to appoint a DPO, appointing an unqualified individual, or failing to provide the DPO with adequate resources.[288] Individual company managers may also be subject to a hefty fine.[289] Additional administrative fines can be imposed against a company pursuant to section 130 of the German Administrative Offenses Act, or *Ordnungswidrigkeitengesetz*.[290]

Though the legal backdrop provides a clear basis for empowered DPOs, our research suggests that it is not independently responsible for the current position and role of the DPOs or for their ability to access and

proposing improvements, monitoring (prior checking), consultation, maintenance of a public index of data processing activities, notifications to supervisory authority, staff training, and complaint handling. *Id.* § 4g(1).

281 The DPO is an independent officer within the firm, but is subordinate to the head of the firm. *Id.* § 4f(3). When using his or her know-how in terms of data protection, the data protection officer is not subject to reprimand. *Id.* Any data subject may contact the DPO to report any violation against data protection regulations. *Id.* § 4f(5). The DPO may contact the supervisory authority to consult about the application of the law to firm practices. *See id.* § 4g. The firm is obligated to support the DPO in her activities, and provide the DPO with sufficient budget, material resources, staff, and access to information and processes, in addition to access to advanced training. *See id.* §§ 4(f)(3), 4(f)(5).

282 *See New Requirements for Data Protection Officers in Germany*, *supra* note 276.

283 BDSG § 4f(3).

284 *See id.*

285 *Id.* § 4g.

286 *See id.*

287 *See id.* § 4f.

288 *Id.* § 43.

289 *See id*. § 44(1).

290 *New Requirements for Data Protection Officers in Germany*, *supra* note 276.

leverage resources in the firm. There is actually a reported under-enforcement of the DPO requirements and a general reluctance from regulators to impose maximum fines.[291] However, as we discuss below, fidelity to the lofty vision of the DPO found in law, according to our interviewees, has recently fully emerged. Its arrival on the scene appears to be a product of both the long-standing legal obligations—historically, often begrudgingly met with the appointment of outside counsel rather than internal DPOs[292]—and the high-profile failures that have been exposed in recent years as increased transparency and publicity have come to highlight privacy failures.[293]

The DPOs we interviewed sat very high up in the management structure. Their status ranged from Senior Executive to Vice President. Every DPO reported regular interaction with the board of directors. Some reported to their board quarterly, others yearly. One discussed conducting "deep dives" on privacy with the board. Another reported on specialized training for board members:

> [Every board member] has just to go through a data protection training with me personally for one hour, because all of the very high[ly] paid people from all over the world are not aware of the conditions we are playing in, and it really makes sense to try . . . to start with this top down approach. And it's not a normal online training . . . . This is 70 people worldwide. Business leader team[s] . . . it's also for the board members themselves . . . one at a time.

Access to the board was a source of leverage and power for the DPOs with which we spoke. For example, one reported working with the human resources board member in the wake of several scandals to develop an innovative program to train the heads of all business units. Some DPOs reported more frequent and sustained interaction with a board subcommittee responsible for privacy. Such subcommittees, along with specific board members responsible for privacy or employee interests were viewed as an important source of influence on firm decisionmaking. As one DPO explained:

> [W]e have this board member . . . [who] is responsible for data protection also which is very, very important I would say. I

291 *Id.* If a noncompliant company has at least gone through the ritual of appointing an internal privacy officer—even if it is found to be guilty of privacy abuse—"it is extremely unlikely that a punishment will ensue." *Id.*

292 *See infra* Part IV.A.2.b.

293 *See infra* Part IV.A.2.b.

> always was of course . . . [in] direct report to a board member. I was in direct report to the financial officer before but since we have this board member for privacy, legal, and compliance it has [added] on top of this and [there is] much more impact on the board itself . . . . They are number driven there and now we have someone . . . asking wait a second. Let's think about the other thing, and this really helps.

Some DPOs considered the independence required under the law, which places the DPO in an internal position but with no accountability to management, to be an important contributor to the DPOs' status and power. One DPO explained:

> The independence . . . makes it []possible to just judge in a very neutral way. It's very important that the function is neutral . . . . We have to be able to stand up against it and say, "[n]o, we read the law like this and we interpret it like this," and we say it has to be done that way. And they, then, have to tell their people how they have to do it so that the real responsibility for keeping data protected and secure is with the respective management.

Some DPOs noted that some firms would choose to appoint an external DPO rather than an internal one to avoid the job security and other protections that gave the insider DPO power—and of course more meaningful access to the firm. One DPO explained, "quite often companies prefer [an] external one, because they believe they could [more easily] get . . . rid of them if they cancel the contract." According to our interviewees, many firms do not comply with the requirement to appoint an internal DPO because it is not aggressively enforced and if discovered poses a limited risk. One estimated that "more than fifty percent of the companies . . . don't have one" but emphasized that it was "not a big risk . . . unless you have a real disaster, like a data leakage or something happens, and then if the authorities would come in . . . then it would . . . cost from €10,000 and who cares?" However, the officers we spoke to view the external DPO role as far less effective, in part because it lacks the independence accorded the internal DPO and the power that flows from the position.

According to our interviewees, the rate of compliance with the German DPO requirement is improving in part due to the advent of new laws requiring companies to disclose security breaches and greater publicity generally about corporate privacy failings at corporations. These public failures generate a connection between privacy protection and brand image, and the DPOs reported being accorded more deference, more authority, and more power within the firm as a result. DPOs, especially those at firms that had been directly affected by a privacy scandal, reported accreting power and growing resources.

In a society that values self-governance, the breach regulations—combined with growing exposure and reputational risk from noncompliance—provided independent DPOs with powerful support for their arguments. "I'm open to say that regulation really helped us," one reported. The statutory framework provided the baseline against which companies would be judged:

> [C]ompanies want to be compliant . . . and so this really helps us also for our argumentation to tell the people there is some kind of regulation which comes out of the fundamental law in Germany and in Europe and we have to stick to this and most of them understand it, of course.

Publicity thus provided the possibility of public shaming, raising the stakes.

b. The Expanding Role and Responsibilities of the DPO

The DPO is envisioned as an extension of the regulator, placed within the company with access to data and decisionmakers, but with overriding obligations to regulators and the law.[294] The DPO's duties, as outlined in law, are generally aimed at supporting compliance and are internally oriented.[295] The independence and distance from management prerogatives provided by law is, as noted above, valued by some DPOs.

The DPO is not legally charged with implementing privacy, but rather with advising on implementation. As one DPO explained:

> [C]ompliance with data protection is the ultimate responsibility of management, either the managing director of [a] legal entity or in our case, the corporate board . . . . The role of the corporate data protection officer and all the people in the data protection organization is to give advice . . . . Of course, on the other hand, business is free, relatively free to decide also against our recommendations.

DPO's reported spending between five and thirty percent of their time on compliance activities, and an additional ten to thirty percent working with legal affairs—which reflects a substantial compliance orientation. Ten to thirty percent each is reportedly spent on business development and

[294] *See supra* notes 281–293 and accompanying text.

[295] *New Requirements for Data Protection Officers in Germany*, *supra* note 276.

government affairs, both of which reflect broader strategic engagement. Corporate strategy, management, and interaction with IT security were other areas in which DPOs reported significant allocations of time. Specific internal activities run the gamut:

> [W]e spend most of our time in consulting the organization [on] what is necessary to be compliant. So our function is really a consulting role and a training role and also an auditing role. So these are the three main areas we have. We have to explain the requirements that come from the law. And we challenge all the ideas we come across in order [to see] how can they be further developed . . . . And we have—that is maybe, hopefully this is sixty, seventy percent of the time we have, we can spend with this. Because this means that our processes of involvement of the data protection officer are in place and work.

All DPOs we interviewed, as required under the law, oversee training for employees. It was viewed as essential to the compliance function, as captured by one interviewee:

> [We train] in order to make people able to ask that question, to be aware . . . that there is a topic and I have to react on that and I have to make sure that I have seen all the issues around that. Therefore we train the whole organization . . . .

All of the firms provided some basic, generally web-based training, for all employees. Each firm reported providing additional training in specific areas defined by job title, tasks or projects, data sets or databases, or country. In addition, many of the DPOs used the firm intranet to provide self-service access to privacy assistance, guidelines, and training, and to disperse other educational materials. Some reported holding workshops and other forums devoted to privacy training.

While compliance played a larger part in the job of German DPOs than in that of U.S. officers,[296] our interviews found that DPOs were often engaged in overseeing compliance activities but also operating at a more strategic level themselves. Like our U.S. cohort, in which privacy leads had somewhat varied backgrounds and training,[297] our German cohort also had mixed backgrounds. Of those with advanced degrees, five were in law and three were in economics. In comparison, Spanish and French DPOs were generally lawyers for whom privacy was just one aspect of managing

[296] Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 265 (explaining that rules-compliance is of limited value to the U.S. privacy regime).

[297] *See supra* Part III.A.2.

legal compliance for the firm.[298]

Given the inward and compliance orientation of the German law, our finding that DPOs are spending an increasing amount of time on activities other than compliance, including a substantial amount of time externally engaging nonregulatory stakeholders, came as a surprise. Like U.S. CPOs, who reported spending nearly half their time on outward facing activities,[299] German DPOs reported spending significant time with external stakeholders. For example, as one DPO reported:

> I personally—I would say forty percent outside . . . forty to fifty percent outside. I would say forty—but not so much internationally, twenty percent, something like this. It's more or less when I go to conferences or I try one of these audits and discuss it with the CEOs, and sometimes I try and—the colleague who is responsible for our international privacy circuits is at the meetings of our international privacy offices in the different regions in the world. Sometimes I go there, too . . . .

Another reported:

> I'm the Chief Privacy Officer of my company . . . [W]hat I do is . . . divide it in two parts. One . . . focusing [on] external third parties like data protection authorities attending conferences, speaking at conferences, working with industry associations with data protection, professional associations and meeting with peers from other companies. The second . . . I think, sixty percent to sixty-five percent of my time . . . [I spend] focusing on internal projects, mostly managing my team doing the privacy work in the company.

Another, estimating how he allocated his time, said, "I would say it's fifty-fifty (external/internal)." Another described his role as split into thirds:

> [O]ne-third . . . is more compliance-related work . . . deal[ing] with human resource records, dealing with contracts, dealing with . . . companies' processing costs and data to all of this legal work, and also support[ing] our IT people by understanding what the local laws mean concerning their protection measures. One-third . . . is . . . more like an internal consultant who work[s] . . . to help [the firm] . . . understand [its] . . . responsibility . . . [T]he last third of my time is . . . lobby[ing] activities.

298 *See infra* Parts IV.B.3.b., IV.C.2.

299 *See supra* note 171 and accompanying text.

With respect to external responsibilities, the DPOs in Germany reported regular, proactive interaction with government regulators, and peers, and, to a lesser extent, civil society organizations. DPOs reported routinely meeting with relevant data protection authorities to discuss new issues, as well as on a somewhat regular basis to merely check in. In the words of one DPO:

> We try to be proactive and we meet authorities. Not all of them but let's say all main authorities . . . on a constant basis, . . . we meet them two, three times a year to talk generally about developments. We tell them, "[l]ook, there's [a] new product we are planning to roll out." Or from earlier incidents where we know that they have a high interest in knowing about changes related to certain issues, then we discuss that with them. And that has been very, very helpful.

The extent of proactive engagement varies depending upon the state of the field—regulatory interest, public concern, and other factors. As one DPO described:

> This really depends whether there is an interest of the authority or the public discussion related to it. For example, if the authority, or also the Article 29 working group has . . . issued recommendations for a certain topic like RFID technology . . . then of course . . . we proactively try to introduce our planning, our product to them. It's not in a sense of an approval, because we're not forced to go[] through an approval, but we want them to understand what we are doing there.

DPOs also attempt to educate regulators in order to mitigate the risk posed by the introduction of a potentially controversial technology or practice. One reported:

> [W]e do a risk analysis to find out if we launch the product, could it be that there would be press reactions on it, which automatically would go to the authorities. So . . . they need an understanding [of] what is it [sic], and the experience says that if they don't know at that time, they—always we get react[ions] [that are] not so positive. So that's what we try to avoid by informing them and then they feel much more secure and they could always and very truly then say, "yes, we have been informed and we are in discussion." And during the discussion we find out whether they have any kind of . . . [problems] with that. And then we see how we [can] work with that. I think by now we have a pretty good [understanding of] . . . where this occurs and where [it does] not.

Another DPO pursued interactions with regulators in order to sensitize them to the challenges facing industry, "go to governments, go to the European Commission, go to data protection authorities, go to conferences and try to explain [to] all of these people where we have original problems." These interactions were generally between the individual company and the regulator. For example, one DPO stated:

> I'm in regular contact with the leading authorities in Germany . . . for example, where we discuss our—on a very concrete basis sometimes—our solutions for the mass market we have. So this is very concrete . . . and it's very important to discuss it with him before so that we know if he accept[s] it or could accept it, this would be a very good support in the public discussion later on.

Another reported "very intensive contact" with the lead authority, reporting meetings "about every six weeks to two months . . . to discuss specific projects or to discuss politics, policies and so on, sometimes also complaints though as we do not have a huge B-to-C business, the number of complaints that the authority receives is fairly limited." Another said, "[i]n general we have close contact with them . . . in case we have some special things we are always discussing." Interactions can reportedly range from merely informative discussions to negotiations. As one DPO described:

> Sometimes we say if a thing is okay, we go straight ahead and [we inform the authority] . . . about this later on because it's an important business model, for example. And sometimes we say [he] can be critical, let's go to him and discuss it with him and convince him. Never go to an authority with a question, always go with a solution.

Sometimes DPOs will use the Data Protection Authority to provide additional weight to their advice to the firm. As one described it, "I will go [to the authority] . . . with the head of the responsible department in my area and sometimes if there are managers in the operational area that do not want to understand what we tell them, we take them with us so that they" can learn something there.

While DPOs seek regulators' advice and input, the DPOs emphasized that it is advisory, not binding:

> [W]e frequently talk with the authority on a very informal level and tell them what we are going to do, how the company is changing. I mean, we are the biggest employer in the whole state . . . and we have dealt with them in the compliance investigation because we had a huge number of privacy related

> aspects to deal with in running that investigation and we developed together with them a system on how to reduce the data, how to limit the amount of personal data that we needed to process in that context but that doesn't result in kind of formal approvals or whatever. Rather, the authority always says "[w]ell, you see, the law doesn't provide for our formal approval so that's why we're not going to give you that approval," which is, by the way, true also for the first set of binding corporate rules that we had. The German authorities always argued the law doesn't provide for a formal approval [by] . . . the authorities so you will not get our formal approval. We can tell you where we are fine with what you do and how you implement that but no formal letter stating that we have accepted this, and that was the situation for many years.

Whether advice is issued specifically to the company or a "common opinion" published jointly by relevant regulators, the DPOs' emphasized "that [it] is of course something that must be taken into account by a company if it is relevant. But still then, you do not have really a binding thing. The only thing that is binding is what a judge decides."

Our interviewees reported that regulators occasionally met with industry sectors. One reported:

> [S]ometimes the authorities themselves offer certain kind[s] of venues. They do that from time to time . . . in the telecommunications sector. Then some federal state authorities do kind of yearly get-togethers with data protection officials, which is also important to see what they're working at and where they have pains.

These meetings were generally closed events. The sort of multi-stakeholder public workshops and meetings that are common at the FTC—which our U.S. cohort viewed as an important part of the development of U.S. firms' understandings of their privacy obligations from the perspective of "social license," if not black letter law[300]—are not part of the German landscape. However, Germany does have a professional association of data protection officers that convenes and educates DPOs and invites in a wider range of stakeholders.[301] The association does not provide certification and training, but it does support information exchanges regarding best practices and policies, and also provides a forum for broader cross-cutting

[300] *See supra* notes 205, 207–208 and accompanying text.

[301] GERMAN ASSOC. FOR DATA PROTECTION AND DATA SEC., *supra* note 277.

engagement with regulators.[302]

Sometimes external engagement is aimed at shaping the regulatory environment, including influencing new laws. For example, one DPO claimed that he is "actively engaged" in legislative debates, and described how his position as an independent actor within the company allows him to speak to the privacy issues where the firm's business interests spoke on the cost issues. That DPO explained, "[y]ou are an independent data protection officer. You are allowed to say something critical, and it worked in there."

Regulators were not the only external constituency identified by the DPOs we interviewed. Interaction with peers and professional groups was routine and valued by the DPOs. Most reported regular participation in meetings, workshops and conferences held by professional associations, as well as less formal interactions with select peer groups. As one explained, "[w]e interact informally, we exchange knowledge. We discuss issues and of course . . . [there] are a lot of organizations that spread information, that try to create certain standards and understandings." The DPOs we spoke to viewed both German organizations like the German Association for Data Protection and Data Security ("GDD") and the Bavarian Society for the Protection of Personal Data, and international organizations, such as the IAPP, as essential venues for sharing information and generating best practices.

DPOs also referenced participating in more general information sharing that occurred between large German companies. For example:

> [T]here is an informal group of thirteen German privacy officers. Most of them are from huge German companies. Not all of them are listed on the stock market but many of the big German companies and we meet kind of regularly on a six month basis and have lots of informal discussions in between. Whenever you have a specific challenge you want to see does anyone have a solution for this and that and so on; it's an exchange of experience and knowledge and so on.

In addition to interacting with professional privacy peers generally, the DPOs also reported regular interaction with DPOs in their particular market sector. For example, one reported being the "head of the Workgroup on Data Protection of . . . a [sectoral] industry association." The activities of these professional associations and networks run the gamut from highly informal meetings to formal workshops and events that include regulators. Some associations are purely focused on information sharing, others

302 *See id.*

engage in lobbying or other action aimed at influencing the policy environment. "You will know that the IAPP, as an example, is an organization that helps to advance the profession but does not do lobbying in the formal sense." DPOs view professional networks as particularly important for smaller companies, because "many of them are—the only privacy function in their respective companies . . . . And that's why . . . the industry associations are quite strong in organizing that exchange of views and we try to share and help each other as much as we can."

DPOs identified peer interactions as valuable because they assist with managing risk by providing access to information and practices of similarly situated organizations. These interactions are useful in clarifying what others think the law requires given its ambiguity. As one said, "it doesn't make sense to reinvent the wheel . . . it's a question of benchmark, or in other words, it could also be the question of what is the proper defense line. The law doesn't give all the answers you need . . . ." Going to peers first was viewed as preferable to engagement with regulators in some instances:

> As a company representative, you would not in a first instance go to authorities because there is a potential risk that they do not take into account the business implications and they simply ask too much. So you better talk to your colleagues and see what you think is possible that we can do, and if kind of all say okay, then let's try this, we have an industry position, which doesn't mean that if something goes wrong people wouldn't say you have to do better. But at least [there is] the defense line saying, "[w]ell, we tried to and look, all the others do the same." So that's, I think the approach behind it.

Professional associations also facilitated the development of shared competencies. DPOs reported reliance on professional connections and networks as they sought to enter or advance in the field. Professional associations support mimetic isomorphism,[303] which is viewed as an important way to manage risk and maintain support for co-regulation. Surely, it must also serve to provide some assurance of shared training and knowledge in light of the competency requirements established by law. Given the absence of specific standards and certification requirements, isomorphism would appear as a particularly important strategy to both the

[303] That is, the adoption by individual firms of structures and practices considered "legitimate" in their field from other organizations like competitors, unions, professions, and trade associations that are. Paul J. DiMaggio & Walter W. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, 48 AM. SOC. REV. 147, 150 (1983).

DPOs and their firms in gauging, informing, and meeting legal requirements and regulator expectations.

Finally, DPOs indicated that professional associations are important vehicles for influencing the external regulatory environment. As one officer told us:

> The associations, I think, are also very, very important. They are part of . . . what I would take into the lobbying area. You go there, you take part in the discussion . . . you get yourself a better understanding of what our potential risks of new legislation are, or developments . . . . I think . . . it's a very good platform to interact and get new ideas on both levels, on the operational side but also on the strategy side. So as often as I can I participate there, and my team members also have the possibility to go to these meetings and exchange point of views.

While some DPOs identified a tension between the pragmatic and lobbying aspects of associations, they agreed that "the majority of privacy officers are no[t] politic[al] people." Their goal in engaging the external environment was primarily, "to find a balanced approach by supporting the business, but also protecting the personal data." Like CPOs in the U.S., they positioned themselves as a bridge between the company and the outside environment.

Despite an overall shared external orientation, in contrast to the U.S. CPOs, DPOs in Germany report far less interaction with civil society and academics than that reported by U.S. CPOs. While one German firm explicitly included privacy as part of its overarching corporate social responsibility program and another indicated that privacy research was part of its research and development engagement with academics, the majority reported little to no interaction with privacy or consumer advocates or academics in related fields. As discussed above, as a general matter German regulators do not facilitate interaction with civil society organizations or academics. Meetings with regulators are typically one-on-one or occasionally with peer firms and the regulator to discuss a cross-cutting issue. To the extent that civil society, industry, and regulators do convene, it is through meetings of professional associations, and, to a lesser extent, academic conferences. The annual meeting of data protection authorities is the notable exception to the general lack of multi-stakeholder engagement.

While engagement with civil society *per se* was slim, our interviewees reported interactions with works councils that were rich and ongoing. They reportedly served as a constant site for negotiation over the practical realities of privacy protection—and its relation to other values—within the firm.

The advisory role of the German regulators, the general predisposition and expectation of corporate participation in establishing what data protection laws require of firms, and the enhanced publicity attendant to privacy failures have led DPOs to allocate a substantial amount of time to external engagement despite a regulatory framework that faces them inward. As in the United States,[304] DPOs actively participate in crafting the regulatory environment. They are then responsible for implementing the rules they have assisted in designing within the firm. But within the firm, as discussed below, they still must negotiate over requirements, as the DPO and the works council, or *Betriebsrat*, representative both must agree on firm data processing practices that impact employees.

c. Operationalizing Privacy Through Distributed and Integrated Expertise

Similar to U.S. firms,[305] German firms integrate privacy into existing risk management functions, aligning privacy with other core firm goals and thereby benefiting from a broader set of resources and structures. Whereas in the United States, we found a uniform decision to distribute expertise and accountability throughout firm decisionmaking, relying on embedded personnel with specialized privacy training and business leads ultimately accountable for privacy,[306] in Germany, we found many firms adopting a similar model but with greater centralized control over policymaking. The greater centralization of control is attributable to the independence requirement placed on DPOs by law.

As in the United States,[307] we found that many German companies favored a system of distributed and integrated expertise. The DPOs work with business units to find appropriate embedded personnel to take on the privacy function. While direct reports—those who report directly to the DPO on privacy—ranged from five to seventeen, indirect reports—those who report to a business executive—and distributed personnel with privacy training ranged from fifty-six to three hundred. Direct reports were typically responsible for business segments or geographic regions. In some instances they were dedicated to a highly sensitive data processing system or process, or to a particular functional vertical such as human resources.

304 *See* Bamberger & Mulligan, *New Governance*, *supra* note 12, at 490–93.
305 *See supra* notes 180–190 and accompanying text.
306 *See supra* notes 189–194 and accompanying text.
307 *See supra* notes 184–190 and accompanying text.

We found indirect reports in various layers of business units as well as in cross-cutting functional units. Some reported only to the business lead, while others had indirect reporting responsibility to the DPO. As in the United States,[308] these embedded players were not necessarily devoted full-time to privacy, but were valued because of their ability to address issues as they emerge in an integrated fashion.

The DPOs we spoke to generally found embedding personnel essential to the operationalization of privacy. The DPOs vividly described the difference between a lawyer sitting in a stand-alone compliance department, and a distributed set of individuals with privacy expertise and responsibility infiltrating business units:

> The people give you the power and the ability to make something . . . to have some structured approach to privacy. You must have someone who takes over the responsibility and discuss it with who's planning and making concepts and so on, and I'm convinced that every privacy officer must have a certain amount of people to be able to work properly. This is definitely . . . the reason why we also go to our subsidiaries and affiliates and tell them that they must have more people there. [If] [i]t's only a few people, it's not good enough. If I want to penetrate business a bit, only a little bit with privacy ideas, I must have people for that, and the people will generate . . . additional ideas, like defining a new process and new procedures, discussing . . . requirements . . . [writing] them down. Who will write them down? When I'm alone, myself? When I started . . . I had . . . twenty-two people . . . I was very alone in an office in the headquarters . . . . All the data-protection people were somewhere out there, and I started to write policies and guidelines. I had one day. I wrote fifteen guidelines and policies, so wonderful. I knew . . . from my job as a lawyer how to draft . . . but they had absolutely no effect, because I had no people who help me to implement . . . [them] and to live it, and this is the most important thing.

With embedded personnel, the DPOs were able to influence the firms' activities in a more meaningful manner. As one DPO stated, "[w]e have to have someone [in the relevant business units] . . . we do workshops with these anchorpeople in order to get them into the topic and work quite close together with them." The DPOs reported that their ability to leverage a distributed set of embedded privacy experts was useful both for staying abreast of developments raising privacy concerns as well as for the process

[308] *See supra* note 196.

of implementation. One DPO described the role of these distributed players in this way:

> [My team and I] define, as an example, the annual goals and we discuss with [the indirect reports] . . . from the sector or the division . . . . The business gets involved in a kind of early stage because we have a system, a risk management system, where we try to identify risks, privacy risks, and that includes kind of formalized meetings and discussions with business representatives in order to, on one side, give feedback on the last cycle. What risks have we identified together with business? How were they dealt with? How were they mitigated and so on. And on the other side, that's the opportunity to talk and then see where's business going. Are there any new fields of business? Are there any other strategic changes that could result in changes?

This DPO also discussed a more recent vehicle for supporting his distributed staff:

> In addition . . . we have . . . regulatory and policy meetings . . . where we sit together in a kind of diverse group on [a] sector level and discuss with sector representatives what is going on, for example, in data protection or in regulation of medical devices and so on.

The DPOs' office provides guidance documents and tools to facilitate privacy work by the indirect reports and other privacy experts within the business units. They consist of "management tools . . . templates, processes, checklists, guidelines, a whole range of nontechnology tools for privacy, [and] . . . privacy impact assessment[s]." These tools were viewed as crucial to ensuring privacy in a large corporate enterprise:

> [P]eople are engaged. They've got the tools. They understand where they're trying to get to. And they've got the right kind of competencies to apply them. In that way, we think that's the best way to work with a distributed community of people, professionally competent and tasked with performing this job locally without going across a whole bunch of policies and so on.

Several DPOs discussed efforts to address privacy during technical design. Such efforts were supported by staff with technical expertise, and used tools such as privacy impact assessments to facilitate an "iterative process" around privacy "where we understand what the product is, we understand its impacts and we find ways to mitigate those impacts, [and where we also understand] . . . the wider legal context in which we may be forced to take a particular decision." One DPO said "[w]e've got this privacy and security assessment, which means we have consultants, [who] . . . are working [on] . . . the projects." Another explained how his firm incorporated privacy as follows:

> We always have two guys, a legal guy and a technical guy. And when we talk about a problem like web tracking, for example, then the technical guy[] says okay it's about permanent persistent cookies. And you don't have to do that . . . . [T]hey're doing consulting in this area the whole day . . . they know what the real technical problems are. And they know the language of the programmers. And so, with this knowledge, they can write down, really, requirements for standardization. And this can be reused every time a web application, for example, is programmed and there is a chance of web tracking . . . . [T]hen the . . . [programmers] can say "[o]h I don't have to use persistent cookies," or "I have to do anonymization."

These sort of processes eventually led to the development of tools for internal use by firms, such as a "large set of . . . concrete requirements . . . for the [software and application] developer."

Though most DPOs we spoke to utilize embedded personnel to their advantage and were extremely supportive of such a structure, a small number viewed decentralizing and embedding expertise as inconsistent with the requirement of independence. As one DPO explained, contrasting his company's approach to that taken by an American peer:

> [I]t makes sense in Germany to have a central data protection unit . . . . We can collect all the people that have some privacy responsibilities under the data protection officer . . . . And he's able to check business models and IT applications, and to give a reliable statement of compliance, let's say that . . . cannot be given by operations, by the open operation of business. So, compared [to an American company], we have not so many decentralized people. In America, it doesn't make a difference I think, decentralized or centralized. They just have to take care [of] . . . the privacy solution. In Germany, it makes a difference because we are the only ones who can say . . . what you are doing [is okay].

Our interviews reveal some tension between independence—which in its most extreme form relegates the DPO to a purely advisory role—and the effectiveness that comes from regular interaction with business units. This tension is dealt with differently within the firms. One DPO with a very rich, larger infrastructure said:

> In the end you are part of the company. You get paid by the company like the Works Counsel too. You have some target management of course and these are all factors that play a certain role within this area but on the other hand the Data Protection Officer is also accepted here in the company, an independent function.

Like in the United States, German DPOs who have pursued a more integrated approach believe privacy benefits from integration because it allows DPOs to be proactive and solution oriented rather than solely concerned with compliance and viewed as the "no" person. An officer we interviewed who utilizes an integrated approach described the DPO position as "one of the most creative jobs in the world . . . . [W]e try to solve these problems and for this you must really have some creative potential I would say."

An exchange with a DPO based in another jurisdiction but with operations in Germany shed some light on the broad range of possibilities under the formal DPO requirement:

> [W]e have one [legally required DPO] in Germany as well . . . [who is] one of these people who represent the regulator within the organization, but . . . we outsourced it, so our link to the regulat[ors] . . . is now via an outsource provider . . . I don't even know the name of the independent outsource guy. I used to be in fairly close contact, so I would say maybe bimonthly basis with the German independent embedded before they were made external under the positions, outsourced to somebody's name I don't even know. I didn't even know that happened until I tried to contact the previous person and was told they weren't there . . . I have no idea [what they do]. I have no link []to them . . . I presume they are speaking to the local lawyers, who I do know and who would then come to me if they need a kind of European view rather than just the German view . . . . I think this person is a compliance person, but I think in Germany they would report—well, I mean they're an outsource provider, but so they would report, for want of a better phrase, to German legal. So the model is not consistent across the organization.

The DPO supports the distributed expertise model, as in the United States,[309] through specialized training. All firms reported regular training, as discussed above. However in addition to basic training for all

[309] *See supra* note 191 and accompanying text.

employees, some firms reported "trainings for specific areas like HR, like IT security, like IT developers, . . . procurement, [and] . . . business security." In those areas firms also "define[d] specific concepts, like investigation concepts for the group business security . . . [and] for the group auditing and risk management . . . . This is very specific and firms we train them also on . . . [these] specific issues." Firms reported that training allows allocation of responsibility for privacy issues out to business units to be feasible.

An additional similarity in the integrated and distributed approach used by firms in the United States[310] and Germany is the common decision to embed privacy in larger structures of corporate risk management, including audit. Each of the DPOs we interviewed reported that his or her firm used both internal and external audits to monitor compliance. Though most adopted audits during that 2000s, one reported that they have been in practice since 1994.

While the DPOs discussed stand-alone privacy decisional tools and processes—such as privacy impact assessments, guideline documents, privacy audits, and others—these were later integrated into larger systems designed to manage corporate risk more broadly. As one DPO said, "privacy is part of risk management and also privacy of course is part of compliance and compliance in our company has a compliance risk catalog and there we also feed in." Integrating privacy into larger corporate structures creates an additional resource. One DPO offered a concrete example of this:

> [We use a] process for development of software . . . systems which . . . already existed where . . . [someone] has to go and has to say I want money. And so we just plug into this process and say "you get your money only if you get our approval." And to implement that on your own . . . from privacy is almost impossible if you don't find this kind of process where you just plug in.

The DPOs reported close cooperation and regular interaction with chief information security officers. They reported joint boards and reporting structures, shared assessment tools, as well as ad hoc committees as needed to address emerging issues. As explained above, all DPOs reported that their firm used internal and external audits to monitor privacy compliance.

B. Privacy on the Ground in Spain

Our interviews with Spanish privacy leaders, and survey of their

---

310 *See supra* note 181 and accompanying text.

responsibilities and practices, reveal a tumultuous external landscape that interacts with Spanish firms' internal attributes to shape the management of privacy. Compliance with data protection law—and, in the shadow of the perceived futility of such efforts, to some extent risk management—drives all firms' privacy activities. Corporations are governed by the Ley Organica de Proteccion de Datos de Caracter Personal (the "PCP"),[311] characterized as one of the toughest privacy laws in the European Union[312] and enforced by the Agencia Española de Protección de Datos.[313] The agency has robust interpretation, investigation, and prosecution powers, including the authority to impose large fines.[314] It is viewed as operating largely unilaterally to establish what is required of firms. The Agency has grown in recent years, measured along any dimension—staff, cases, and penalties.[315] It is the touchstone of firm privacy activities.

This shared definition of the substantive task of protecting privacy translates into an initial set of shared structures and practices across the firms. These structures and practices are predominantly subsumed in broader legal compliance activities and are internally focused. Within these broad contours, however, we found greater variation across firms than was evident in the other countries under study.

Interviewees agreed that compliance is the primary objective, and also that it was difficult to achieve. Interviewees' perspectives diverged on exactly what complicated their efforts to comply, and whether the complicating factor(s) can be effectively managed. The difference in viewpoints led privacy leads in one set of firms to have a greater external orientation, while in another it led to somewhat more extensive efforts to move privacy throughout the firm with decisional tools more akin to those found in U.S. and German firms. The firms reporting a higher level of external engagement described a very unpredictable environment where a largely political agency wielded power to exact fines from firms within easy reach. The agency's power was also invoked at the whim of

---

[311] Spain's first data privacy law was enacted in 1992. *See Constitutional Privacy and Data Protection Framework*, PRIVACY INT'L, https://www.privacyinternational.org/reports/spain/i-legal-framework (last visited June 9, 2013). The 2000 PCP law is also referred to as the Data Protection Act (LOPD). Lisa J. Sotto et al., *Information Security and Privacy: A Practical Guide to Federal, State and International Law*, 2 DATA SEC. & PRIVACY L. § 11:203 (2013).

[312] IAN C. BALLON, 2 E-COMMERCE AND INTERNET LAW § 26.04[12] (2012); NORTON ROSE, GLOBAL DATA PRIVACY DIRECTORY 41 (2012).

[313] *See* NORTON ROSE, *supra* note 312, at 41 (explaining that the Spanish Data Protection Agency interprets Spanish privacy legislation through resolutions and reports.)

[314] *Id.*; *see also* BALLON, *supra* note 312, at § 26.04[12].

[315] *Id.*

consumer groups, unions, or other civil society organizations as part of a larger battle against companies. The firms that emulated the privacy structures and expertise they attributed to U.S. firms expressed dismay at the growing bureaucracy they faced in the privacy area, but did not view privacy as politically volatile. As a result, those firms are more practically oriented. They are busily setting up processes and structures to manage their exposure. A final set of firms described a largely inward facing bureaucracy, drafting an intricate maze of specific rules, compliance with which is unfathomable and unattainable by corporations.

While our sample size is too small to generalize, we note that these different perspectives related to specific features of the firms.[316] Firms in industries with high consumer contact perceived the external privacy environment as highly volatile and somewhat political ("group 1"). They doubted their ability to thoroughly address concerns raised through the regulatory process, in part because the complexity of the rules leaves ample opportunity for mistakes, and in part because the privacy field is at times invoked to address other concerns due to the substantial powers of the Data Protection Agency. Firms in highly regulated industries perceived privacy as bureaucratic, but subject to erratic and sometimes punitive use—there was simply no doubt that they would be found in violation of some arcane rule if a regulator chose to examine them ("group 2"). Finally, companies loosely grouped as "high-tech" were prone to be pragmatic in their approach to privacy, viewing it as a legitimate social concern that could hamper their business if not appropriately handled. This last group appeared less driven by the particular proclivities of the Spanish regulatory environment and instead focused more globally on the ongoing dialogue about privacy in a networked society. They were more connected and driven by the practices of their peers around the globe, particularly those of professional associations ("group 3").

As one would imagine, a firm's perspective on the external environment distinctly imprints on the corporate form. While across the board privacy infrastructure was well below that found in Germany and the United States, in some firms—those in groups 1 and 3—the DPOs interviewed were working to bring privacy out of the shadows of the legal shop and seeking to exercise greater influence over business practices and processes. Those in group 1 engaged regulators more proactively, seeking to build relationships that would temper the consequences—fines and

[316] If salient, these connections may further suggest the multitude of ways in which nonregulated parties can be empowered by administrative choices and the extent to which the power they wield advances the values the regulation was sought to protect or is channeled toward other ends.

public approbation—that result from complaints and investigations. They responded to a volatile environment through greater engagement with the Data Protection Agency. This occurred despite limited opportunities and a lack of historic participation and collaboration with the Agency. In contrast, the firms in group 2 viewed privacy relatively narrowly as a compliance matter and did not seek to alter the settled model of privacy, which viewed privacy as a legal affair addressed in the course of business through the work of the general counsel's office. Finally, the DPOs in group 3 sought to integrate privacy into the activities of business units to avoid being the "no" person and to reduce the costs of retrofitting due to legal requirements. The DPOs in this category were often empowered by a CEO and were more connected to professional associations, which they drew upon to develop practices and policies. Thus, unlike Germany, France, and the United States, where large firms perceived as leading on privacy presented a single archetypal form, Spain presented a fractured picture, reflecting, in part, we believe, both recent changes in privacy regulations—specifically the relatively recent increase in the discretion of the Data Protection Agency and its ability to impose substantial fines—as well as a less staid overall legal environment.[317]

In general, the status of the DPO is lower than in Germany and the United States, staffs are smaller, connections to the board are weaker, and connections to firms' functional and business units are attenuated at best. Even those firms seeking to push a more integrated approach to privacy are very far from achieving the staffing, infrastructure, and buy-in required to reproduce what their German and U.S. peers command. While a few of the firms have overarching privacy policies to guide corporate behavior, the law, rather than broader company policy, remains the focus of the privacy task. There is little effort to decentralize privacy decisionmaking or to empower employees to identify and address problems during the work cycle. While some training is provided, it is not necessarily provided to all employees, nor is it generally coupled with broader awareness or educational programs. Generally only a small staff of experts—often in legal affairs or compliance—is responsible for privacy issues.

1. *The Definition of Privacy: Compliance*

Compliance and, given its difficulties, risk management animated the

[317] As discussed above, Spain's first data privacy law was enacted in 1992, while those in the United States, Germany, and France date back to the 1970s. *See* BALLON, *supra* note 312, at § 26.04[12]; Bignami, *Cooperative Legalism*, *supra* note 270, at 422; *Constitutional Privacy and Data Protection Framework*, *supra* note 311.

DPOs. Unlike in France and Germany,[318] there was little reference to human rights, or to the broader concept of private life. Although some viewed consumer organizations and unions as involved in pressuring companies on privacy issues, that rarely translated into a definition of privacy within the firm that focused on those constituencies. This seems to reflect the belief that consumers and employees invoke privacy opportunistically to turn relatively more mundane customer service and employment disputes into broader battles that engage a powerful regulator and stir the public's imagination. A few DPOs identified loss of consumer confidence and the market as motivating factors, but it was in a more generalized, amorphous, and political sense than in the United States or Germany.

The focus on compliance with data protection law was ubiquitous. As one DPO stated, "I am responsible for data protection, as it is known in Spain." Elaborating, another explained that compliance must be assured in internal processes as well as external relations:

> [M]y job is mainly to comply with the Spanish law and to deal with the problem of international transfers: . . . two different . . . roles. One in the back doors, internal management of workers' documentation and information, and the other one with external products, clients and customers, and so on.

This compliance mentality, according to the DPOs, produces a reactive mindset toward data protection. As one explained, "[b]ecause we were going to be fined. It is the main reason in Spain to appoint somebody to data protection. 'We have a problem and we are going to be sanction[ed], so . . . .' It is a reactive manner of hiring someone." Another DPO said that "in Spain, breaches of privacy are very heavily punished according to law and there are serious monetary . . . consequences. So obviously we spend lots of time so as to avoid any claims on breaches." Some were hired as a direct result of a breach: "I was hired for this specific case and then they decided to continue, because I held training sessions with the Executive Board and explained to them these issues about privacy and data protection and that we have to comply, and they agreed."

Even within the firms that were moving beyond a strict compliance mindset, as discussed below, DPOs emphasized that compliance was the first motivator. For example:

> [Compliance] was the first step because when we joined the company, the most urgent, the most—the most dangerous factor

318 *See supra* Part IV.A.1, *infra* Part IV.C.1.

> that we have to handle . . . was compliance on data privacy because as you know probably in Spain we have one of the . . . strongest data privacy law[s] in Europe.

One DPO explained that while they strived to move the company away from a compliance mentality, they had not yet succeeded:

> I think that historically compliance [has] . . . been the driver of information security . . . . I would like to say another thing that now the maturity level of the company [has] push[ed] this company to make a lot of efforts to protect data. It is not all the truth.

Despite a compliance oriented definition of privacy, and the best efforts of the firms, there was a widespread belief among the DPOs that, "[i]t's almost impossible [to comply] 100 percent with all of the requirements of the law." Another simply stated that despite "doing everything," it "is difficult is to avoid a fine." For some, the futility arose from the complexity and density of the rules. As one DPO said:

> There is only one little article in relation to software, but it is very diabolic, as you have seen as regards the Spanish law. And it states that every software for the management of personal data has to comply with security measures, and we have a list of security measures. And I do not know of any company in Spain that complies with it. I repeat, in our training sessions, I challenge the assistants and tell them: if you find any Spanish company that complies with it, just tell me.

For others the dense nature of the law meant, "it's impossible to comply with everything because in math risk, zero risk is cost infinite . . . . So we [evaluate]in this what percentage of risk we decide to face, and what are the risk[s] that of course the company, not us, the company [will] accept, too." Another DPO described a very clear way in which this risk was managed:

> [I]n the dashboard for data protection we have a thermometer where we can see [how] we are comply[ing]— . . . we're right now [at] eighty-two percent that for me compare[s] . . . with the benchmark which we have [which] is . . . pretty good, but it's eighty-two percent, so we know that we have another eighteen percent [of which] . . . we are assuming risk.

This thermometer, "match[es] business process with [the] article of data protection law."

Another DPO explained that the lack of consistency across European jurisdictions compounded the problem: "At the end, it is impossible to comply with everything because the structure, your infrastructure, your technology, is not so flexible that you can scratch all you want. You want red, red, for you, green, for you, yellow. Then I'm expected to manage this?"

DPOs expressed concern with the situation in Spain. Some claimed that the law undermined the competitiveness of Spanish firms: "In Spain, you cannot do business if you want to comply 100 percent with Spanish data protection law. So this is a barrier, a competitive barrier for us if we want to—if we compare, as we say, other non-European companies that target European citizens . . . ." His colleague responded, "yeah. That's an important thing. You can do business within Spain but to . . . compete with people outside of Spain is where the law becomes a big problem." Another officer, discussing the registration and authorization requirements for international transfers, combined these sentiments, explaining:

> [T]he European system is absurd. The European system is very hard. Our system is not adapted to current times and the pace of technology [in the international transfer procedure] . . . you have to explain everything continuously . . . it is not clear to them and they ask for more documentation, and you could make all this with a simple click. DPA [Data Protection Agency] uses a long time to authorize you for something that could be done with one click. That is the reason why most companies do not declare international transfers. They take the risk.

For others, the futility of compliance rests in the broader political and social context in which it is invoked. As one explained, "I would say that in Spain we are—there is a bad . . . use of privacy. What I'm trying to say is that sometimes people see in privacy an opportunity to get compensation, to get money compensation." Consumers and consumer protection organizations were the actors whose motivations DPOs questioned; however DPOs also viewed the regulator as, at times, reluctantly complicit. As one DPO explained:

> [T]here are some claims that in one way or another one can easily see that the reason [behind] consumer[] association[s] . . . is [to] tak[e] advantage of a mistake in order to obtain money compensation. The Data Protection Agency is at the same time aware of this, of this manipulation, but they have to comply and work within the law.

Another noted that the political and bureaucratic nature of the DPA's office is problematic: "the Director is a political appointee and people working there are public servants and they are not passionate about data protection, they do administrative work."

The extent to which DPOs considered compliance a realistic metric for success was heavily influenced by external factors. Corporate conceptions of their ability to achieve compliance with data protection law varied dramatically depending on aspects of the firm's history. Those that were high-touch, business-to-consumer businesses were far more sensitive to pressures from labor and consumer protection organizations, as were firms with high consumer contact. As one DPO told us, "[i]t's our global protection to the consumer but this protection goes from attending personally [to consumers] and . . . to inadequate protection of the information." Expanding on the connection between customers and the vagaries of enforcement another DPO said, "there are some companies that you know [will be targeted], like telecommunication providers, banks, insurance companies, they are the usual suspects. When you have 10,000,000 customers, you get complaints. They go to the DPA. There's investigation. And typically there's a finding." From his perspective, the sheer numbers combined with the mass of rules meant that:

> [T]hose companies . . . tend to . . . typically pay, it's like a tax . . . they know that they have to allocate some money at the end of the day because there's no way you're not going to mess up if you . . . have 10,000,000 customers and you're doing all sort of things with their data.

Another explained that privacy was taken up in the context of sectorally oriented consumer organizations that, "focus on different sector(s), for example, telecommunication, electricity, gas, [a]irline . . . . They are very aggressive in the policy." This further explains why different industries perceived privacy as more or less politically driven.

Subsumed in broader consumer and labor squabbles, the corporations viewed privacy claims as, at best, weakly correlated to actual public concern with privacy. They were viewed as unavoidable and generally not substantive, at least with respect to privacy. The lack of moral weight the corporation attributed to the claims gave these claims little salience within the corporation. This is evident in the lack of influence they have had on privacy's definition within Spanish firms. The actions of civil society groups, unlike in the United States and Germany,[319] neither nuanced or broadened privacy's definition or the DPOs role. The activities of civil society groups did, however, inform the companies' general stance toward compliance—feeding into a more risk mitigation or tax-like mindset. Unlike in the United States—where the activities of privacy and consumer

319 *See supra* note 208 and accompanying text.

organizations, along with media, played out against a legal backdrop that centered on consumers and their expectations in the question of compliance[320]—or Germany—where the works council was viewed as legitimately addressing privacy concerns[321]—in Spain, the activities of consumer organizations did not have a forum through which to influence corporate perception of privacy's definition. Regulators did not convene multi-stakeholder groups to discuss privacy requirements or new threats. As one respondent explained, the role of consumer organizations was in activating the regulator—"the consumer association has big power, and they have a very close relationship with the administration . . . the local regulative administration . . . because . . . [they have] the capacity to initiate the process . . . before the administration, etc. etc." Their role is not in defining the substance of the law.

2. *Shortcomings of the Compliance Mentality*

Although compliance dominated the perception and, as discussed below, practice of privacy, the DPOs viewed this as problematic for several reasons. It keeps the DPO, and privacy, at arms-length from the company, frustrating efforts at achieving deeper, systemic integration into firm processes. Relatedly, it leads firms to choose simple solutions under the law, rather than engage in more meaningful analysis that could lead, according to the DPOs, to better and more cost effective solutions.

a. *Frustrating Efforts at Integration*

Some DPOs believe the compliance orientation relegates them to the role of legal technician hindering efforts to protect privacy:

> The problem is that . . . companies think of data protection first as compliance, and second who is in this: the lawyer. And the lawyer is inside his office, and I always give the same example. I know a lot of lawyers who do not know the software . . . they have to go out of their rooms and go and see. But the concept is this: it is a lawyer thing . . . and we do not care about it. It is very frustrating. And maybe that is why we do not develop good privacy like in the . . . [United States], because we are lawyers we do not get out of our offices to see the business and the thing is that privacy has got more implications than comply, comply, and comply.

The DPOs reported compliance as problematic because it allows

[320] *See supra* notes 148–151 and accompanying text.

[321] *See supra* Part IV.A.1.

privacy issues to be easily dismissed by the business units. As one officer explained "normally, you don't do any more than the law requires . . . . Okay. Because . . . you want to sell products." Compliance also fostered a negative perspective on privacy's relationship to firm objectives:

> You want to make easy the life of [the firm]. All of . . . [the] requirements of the law normally [say] . . . stop it, stop it, stop it. No, no, no you don't have to do it. No, no, no stop wait I have to check it. No, no, no, oh my God this is impossible, stop it now.

A DPO from the high-tech sector aptly explained the downside of being in legal:

> [I]n other companies in Spain the legal is no one. You never go to the legal . . . if you go . . . he's going to say no, impossible. And that's why . . . my boss, put me in the senior management team because it's the first time that I . . . [saw] a chief privacy officer and a legal in this team. And that drove home to people the importance of privacy for the company, the fact that the CPO was at the highest level of the company.

This DPO attributed their distinct position within the firm, and a similar noncompliance focus at his prior employer, to American influence. As that DPO explained, , "maybe that's why . . . the title was [chosen] by the CEO . . . . He said, I want you to be 'chief privacy officer.'" This suggests some level of mimetic isomorphism, as policies diffuse in the private sector from the United States to the E.U. private sector.

b. Frustrating Systemic Approaches to Privacy

Some of the DPOs, particularly those in the high-tech sector, reported that the focus on detailed external rules reduced the extent to which companies felt obliged to wrestle thoughtfully with privacy. One reported: "Many companies . . . just sign on the dotted line and you have compliance designed. Now in other countries where the rules are not so clear then you have experts . . . thinking in terms of security; so this is [what] . . . we want to achieve." One DPO offered the different specificities of the German and Spanish laws as a case study:

> [T]he security provisions in the German law, that's an appendix to the law . . . . It's just like ten bullets. It's much less detailed than the Spanish rule . . . you spend more time discussing about security in real terms with a German customer than with a Spaniard . . . in Spain the tendency is typically you just agree to comply with the law and I don't want to hear how you do it. I don't really want to see your security document. I don't want to

> enter into details. You said you would comply, that's all I want. Germany I would say it's by far the country [where] we get more and more discussions, more detail and thorough[ness].

Echoing this concern, another explained that with law and the lawyers leading, "the privacy discussions can become endless." As a result, "I don't think that they [the business people] really understand why . . . this [is] so important. They just feel it's lawyers talking about stupid things." In response, he said, businesses look for simple solutions to complex challenges such as cloud computing: "So when they realized there was going to be a data center in Europe they said 'Okay, our problems are solved. Finito. It's done.' No more privacy issues. The data is in the European Union, you know, finish[ed]." He pointed out that this focus on legal compliance elides serious issues, explaining, for example, that with cloud computing, where the data resided did not resolve the privacy issues:

> [We had] Indian engineers, Egyptian engineers, Chilean engineers, American engineers accessing the system. So instead of going to the United States they go to [country X] but the problem is the same: [d]ata might be accessed by people outside of the European Union, the same people. So we are not creating a bunch of specialized individuals working in XXX for data center.

He blamed the compliance mentality for steering his company toward an inefficient and less privacy protective—but easily understandable—solution.

In one particularly detailed discussion of the drawbacks of a lawyerly approach to data protection, an interviewee compared company behavior across jurisdictions, explaining that

> [i]n the U.K. . . . large companies . . . bring in a specialized law firm. They don't have this person in-house. They are ready to spend a significant amount of money [on] an external law firm to participate into [sic] the privacy discussion. That's something you can also see in Germany.

In Spain, by contrast, they rely on "clear written rules," which "does not amount to better privacy or better security" because it provides "a false sense of protection . . . customers are very happy with just saying to you, comply with this . . . . That's all I want for you. The law says you [must] comply with it, and we are all happy with it.

3. *Operationalization of Data Protection as Compliance*

While Spanish firms were overwhelmingly oriented toward compliance-focused data protection structures predominantly situated within the legal and audit divisions of the firms, the variables discussed above—high-tech, or in close contact with consumers—consistently exerted some force on the shape of privacy's institutionalization. In particular, within the formerly public and high-touch business to consumer companies we found DPOs to be slightly more senior and externally oriented. Within the high-tech sector, we found DPOs more actively attempting to diffuse privacy throughout the business units as part of daily practice rather than relying on episodic interaction with the small team of privacy lawyers. However, lacking the seniority of their German and U.S. counterparts, their efforts to do so were relatively nascent and modest.

a. Role and Position of the DPO

As with our U.S. cohort,[322] the privacy leaders interviewed come from firms that are heterogeneous on every metric except size. Most have a global presence, although the extent of their international operations varies. Some are highly diversified, others have a single core business. Most of our interviewees come from data intensive businesses.

Unlike our U.S. cohort, where privacy leads had somewhat varied backgrounds and training,[323] the majority of our Spanish interviewees were lawyers by training. All but one DPO had a legal title of some sort. Some reported to a lead legal counsel while others reported to a senior corporate officer at the vice president level or above. Despite the reporting structure, which was somewhat similar to the United States and Germany, the titles of the DPOs[324] were generally less senior than those found in both of those countries. This lesser status was evidenced directly by less access to the board and less involvement in strategic decisionmaking.

Unlike German law, which requires the appointment of a DPO and tasks them with both educating employees on data protection and providing compliance advice to the firm,[325] Spanish law has no affirmative requirements that direct employee training. We found that training is still prevalent, however, although less robust and tailored than in Germany and the United States. Some firms bundled privacy training into information security training that was conducted by another department, one outsourced it to a vendor that provides overall employee training. Notably, the high-tech companies reported more tailored educational offerings—for example,

---

322 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 264.

323 *Id.*

324 Two senior executives, two directors, two managers, and one associate staff. One described his role as "'Consultor', in Spanish. In English, it is consultant. Here, middle managers are consultants. Consultant Manager, for example."

325 *See supra* notes 284, 281 and accompanying text.

providing training for specific job classifications. One reported, "I have a complete system for every employee. Every employee has a specific programme of data protection adapted to their job." Another, explaining his layered approach to training, said:

> When a new person is hired, since we have a general training plan in place . . . everyone who enters the company receives their own training on privacy, for instance, people from marketing. They are the most dangerous boys . . . because they are continuously sending emails and doing telemarketing.

One high-tech sector DPO credited his interactions with U.S. colleagues through a professional association for expanding his perspective on privacy education, "as regards training, I learnt from IAPP. The [Spanish] law does not oblige you to have a training plan, so be careful because what I do here in my job is not typical."

Spanish DPOs' relatively weaker position was evident in their infrequent interactions with the board and little direct knowledge of how often the board discussed privacy issues. One explained: "Normally, the person who reports to the board of directors is the general counsel. And if there is a technical issue, [it] probably is the CFO or directly the I.T. director [who] report[s] to the board of directors because, just below the board of directors, there are different committees." Again in the high-tech sector, more interaction was reported. For example, one DPO explained yearly four-hour training sessions and a monthly newsletter were used to increase the firm's awareness of privacy issues.

The DPOs credited information about breaches and fines for raising privacy's profile with the Board:

> [T]echnology and information security . . . are very, very out of the range of the executive culture . . . which is the composition of the boards . . . . The best way to sell to this person is with [an] example, [a] practical example that happened in the real [world]—and that you have read in the newspaper.

Another DPO echoed this strategic use of press reports stating, "something like WikiLeaks for the data leak prevention project is very, very useful because board[s] understand the importance, the criticality of that." Likewise, one DPO explained that news was an important determinant of whether the board heard about privacy at all, explaining that in general "[t]hey are thinking, the board, in other things, not in privacy" unless it is "in the news when something wrong is happening." He said "[t]hey just want to avoid the penalties and . . . not be exposed to the press . . . [for] doing those bad things with their customers." Another, who attributed his hiring directly to a complaint against the company, said the key thing for the CEO was:

> To get rid of the problem . . . . He told me: 'if I could destroy it immediately, I would destroy it. If I could press the button, here, I would press it.' It was in this room. But the first task was to get rid of that problem at that moment.

He went on to explain that the fine (€30,000) was not what mattered, rather, "the impact in the press would have been bad." He then generalized about Spanish companies:

> [They] have to comply, but [not] only in order to avoid sanctions, in order to avoid fines. They do not want to be in the newspapers. I think that is the only reason right now in Spain . . . it is because of the public sanction [i.e., reputational harm]. Because they have enough money to pay [the fines].

b. Rule Bound and Isolated

Unsurprisingly, given the definition of privacy and the placement of DPOs within the firm, the Spanish DPOs reported spending much of their time on legal or auditing-related work. Many of the DPOs we interviewed are legal counsel who spend only part of their time on privacy issues. Of their privacy responsibilities, the DPOs reported spending from twenty to fifty percent of their time on compliance, and, for most, another thirty-three to fifty percent of their time on legal affairs. This sits in stark contrast to Germany, and especially to the United States, where the CPOs we interviewed were supported by legal counsel who specialized in privacy, but were also themselves involved in high-level strategic activities.[326]

As part of the legal counsel unit, most of our interviewees reported relying on the general legal review required for new products, business relationships, and other corporate changes to identify and address privacy concerns. DPOs described their firm practices in the following ways: "Whenever there is a new project they are obliged, according to procedures, to report to me, to inform me." As another DPO described:

> [T]he normal process . . . the communication department or sale department . . . they consult [at a] . . . very, very preliminary stage . . . about this idea . . . . [I]f the minimal requirement[s] according to the law are accomplished, the second step is to consult with the IT department . . . to develop . . . different tools to implement this idea . . .[Then] probably the matter [will] come

326 *See supra* notes 162–167 and accompanying text.

> back to the legal department . . . [It] is a very dynamic process . . . .

The DPO explained: "We have internal procedures . . . . I am informed whenever he decides to . . . develop the product. I am completely into the assessment during the process." Describing the work of his office, one DPO said:

> [W]e must try to understand all the requirements of the [law] . . . . In each country we must comply, and we must translate this requirement in operative requirements . . . with the legal department of each—of [each] central legal department, corporate legal department, and with each . . . local legal department.

Very few firms had formal processes, separate from the standard legal review, to address privacy concerns. In a striking departure from the norm we found in the United States and Germany, where a key element of corporate privacy management was the adoption and focus on operationalizing a set of overarching corporate privacy principles,[327] the DPOs we interviewed in Spain rarely mentioned corporate privacy principles. Those who used the term did so in a vague and aspirational way. For example, one said:

> I always say I am always away from the law, not because I [do] not follow the law. ..The law is getting really old for me, so I have to follow principles, so I had to follow all the—had to pause the principles to be all the—all my projects to be [in] accord[ance] with the law.

One Spanish DPO working for a subsidiary of a U.S.-based company explained in a roundabout way the benefit of overarching corporate principles given the state of the law:

> [W]hen we receive these policies [i.e., overarching corporate principles], we adopt [them] in relation with internal rules in Spain and the law in Spain, no, but it's very easy because the internal policies in the [United States], in [country X] . . . are more intensive than our relation in the law because the law is more general. In some aspects, no? Because, for example, in quality, [there] are more important . . . rules in the law, but, for example, in safe[ty], in security . . . [there is] more detail in the internal policies in . . . [country X].

327 *See supra* notes 151, 158–162 and accompanying text; *supra* Part IV.A.2.

c. Distributed Accountability

Despite the relative lack of business units' involvement in defining privacy objectives, or means to achieve them, business accountability for privacy, as in the United States and Germany, is the responsibility of business leads. The Spanish model is, however, quite different. In the United States and Germany, there appear to be more efforts by CPOs/DPOs to establish a shared view of requirements through conversation with the business.[328] In Spain, the DPO generally acts as a lawyer telling the business units what they may and may not do. One DPO in the high-tech sector described a distributed system of responsibility coupled with technical detection mechanisms to identify bad behavior:

> The Director of the Area . . . has to comply with the instructions . . . we have a whole system prepared to detect the possible violations, like sending e-mails with information that you do not have. We help them with technical systems, with some information of some technical systems, with other information, it is completely impossible. But directors and managers are completely sure about what their responsibility is.

Acting predominantly as lawyers, the DPOs realize that the ultimate decision is not theirs to make:

> This is a business. Sometimes the best friend of the business is not the regulation, okay? Probably if they decide to implement new products, it's not sure that the final result will be according to the law. We try to advise them, "Okay, there is a risk but . . . it's a business decision."

d. Beyond-Compliance Initiatives

Beyond-compliance models of privacy integration were evident in some firms. Uniformly, they were attributed, at least in part, to substantial high-level buy-in: "it's really, really important, and the CEO, of course, thinks that it's really, really important . . . . If we don't have the support from the CEO, we would not be able to work." The two DPOs whose companies took a more expansive view of privacy's place in the firm both pointed to a significant U.S. connection to explain it. They were also both in the high-tech sector. One DPO explained the influence of his firm's American connection on how the firm thought about privacy:

> Privacy is in the base, it's in the crown of the foundation of . . . [the company]. This is one of the pillars of the company. [Senior

[328] *See supra* note 191 and accompanying text; *supra* Part IV.A.2.c.

> management] believes that the protection of the user's data, of the privacy rights of the users is the most important thing of the company. As a matter of both business and privacy matters. Because we cannot do anything for the business if the privacy of the users is at stake.

The interviewee, perhaps unsurprisingly, reflected definitions and goals more aligned with those of U.S. firms. However, the interviewee's operation and practices were more consistent with Spanish firms. For the other firm, the arrival of a senior U.S. employee was viewed as seminal:

> I think North Americans are more sensitive to privacy issues and he was in [an American Company] and [the American Company] was one of the first companies to have a chief privacy officer. So the CPO role really came when you brought him in. And so it's kind of a vision from the top . . . . It's a vision from him because even in the general secretary of the company and general counsel of the holding at the same time, we were in a retreat the last week. And I had to make a presentation one year after because when I was hired I was working in [the firm] for seven years.

i. High-tech Companies Were Beginning to Adopt Strategies to Socialize Privacy Throughout the Firms

Although the high-tech companies engaged in activities beyond compliance shared the small and centralized staff of other firms, they were more aggressively attempting to produce guidance documents and decisional tools specifically about privacy and directed to various parts of the company. One high-tech DPO described the maze of documents his firm has generated to drive compliance throughout the organization as "the castle"—"a castle with a lot of documents, documents that have developed our law and . . . regulations. As we have a specific law on e-commerce, for instance, not only data protection, and we have also to comply with it and it is all mixed." That DPO explained:

> In "the castle," I have different documents that I sen[d] to different departments . . . to the marketing department, or to R&D, and these documents are continuously being revised . . . . Everybody knows there is an instruction and everyone knows, for example: if I am a marketing person I have to follow this instruction.

This DPO from the high-tech sector was attempting to create a set of decisional tools that would spread privacy thinking throughout the firm.

The DPOs in the high-tech companies communicated a strong belief that effectiveness is tied to understanding the company and that doing so required them to get out of the law office. One explained that regularly interacting with the business units was the difference between an expensive retrofit to address legal compliance concerns and a product built with privacy in mind. Discussing his interaction with the firm's research and development department, that DPO said:

> I had to present myself and say: "hey guys, we have some rules to comply [with] and your products are the machines that treat data and so I ask you to take me in the first stage of your development . . . of your ideas," because it is very difficult for us to adapt a product once it is finished. In 2007 we had this problem, we had to open it and work back . . . now, we take that into account. We follow the rules, and it is very easy.

Another DPO explained:

> I use[d] to loose [sic] or miss a lot of details that were important and now . . . [I attend] technological meetings and for me it is very important. It is one of the best experiences I have had here: knowing the software and knowing how it works. It is very, very interesting. And I assess them to [ensure they] comply with the law.

While Spanish firms are still oriented around compliance, these interviews reflect efforts to integrate privacy into firm activities at a deeper level. These efforts are in part driven by a desire to avoid the costs of retrofitting products and processes, and to avoid being the "no" person.

ii. Engagement with the Privacy Field

In contrast to the United States and Germany, privacy protection as a professional field is far less developed in Spain. Some DPO's reported little to no interaction with other professionals in the field. One interviewee lamented, "it is very strange having only 200 people who are associated [with privacy associations] in a market of 2 million companies, only 200 people, it is frustrating." Some expressed concerns about the lack of professional standards for the DPO/CPO role: "there is no standard definition . . . . And it is scary. I am scared of this because they need to explain more in detail how it works."

Despite the relatively low level of participation in privacy professional associations and sparse reliance on peers reported generally, DPOs in high-tech firms are tightly connected to an international network of privacy professionals. Their efforts to develop beyond-compliance models for privacy work within the firm drew upon knowledge gleaned from professional contacts. They found regular interactions with their peers crucial to their work: "it is very helpful because we share the same frustration and we have a lot of ideas." They found information from peers particularly helpful due to the political, rather than expert, nature of the Director of the DPA: "we have the problem that so far none of the Spanish Directors of Data Protection [Agency] were experts in the field, they were political appointees." For those who reported information sharing among peers, they considered it key to understanding issues and developing corporate responses.

iii. External Forces Expanding the DPO's Role

While our interviewees considered a forceful CEO an important predicate to moving beyond compliance and out of the law office, external forces also raised the level of attention a firm devoted to privacy and created more latitude for the DPO. Interviewees credited the increase in the fines that can be assessed by the DPA with raising the significance of privacy and the stature of the DPO within firms. As in the United States,[329] the monetary loss was viewed as less important than the potential injury to the brand caused by negative publicity. As one DPO explained, "if [the company] has trouble regarding data protection in their reputation, the damage could be very, very practically definite. So I think they are willing to make an important effort to develop a good product." The increased fines garnered significant press attention, thus raising the potential impact of a breach or violation on the company's image. One DPO stated:

> This is a very important topic for the name of the company because . . . not only is [it a] very expensive penalty. But there is an immense damage for the company because [customers feel] you don't take care . . . [of their] data as [a] customer . . . . So we are very [careful] to maintain the legality o[f] our business about data protection.

While the sense that the increased fines contributed to firms' improved attention to privacy within the firms was widespread, the knowledge of other companies' problems was most actively used by those DPOs who were trying to break out of the compliance mode. DPOs explained that publicity about a privacy failure in any country was useful particularly if the company being taken to task was a competitor:

> When you can show something that's happened to your competitor, on one side you enjoy it, and you say, "Yes, better him than me," but then . . . [y]ou mind about it because yes, but if

329 *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 293.

> this happened to my competitor that ha[s] the same structure, environment, business, this can . . . happen to me.

Our interviewees also attributed positive investment in securing data in Europe to U.S. security breach notification laws. As one DPO told us:

> I would say that's been most driven by . . . U.S. evolution, rather than by E.U. evolution . . . [W]e ha[ve] many companies that either are subsidiaries of U.S. companies or have significant operations in the United States and they are very sensitive to all, for example, all the changes in the little landscape in the United States around data breaches. And this has created [a] sort of feeling that failing to protect the data can really cause problems. I think that [in] Europe, and we know that there is [sic] some changes coming probably soon due to the [draft E.U. regulation], but in Europe typically, if there was a breach it was something kind of kept within the company, not disclosed to third parties, managed internally, little noise. The regulators were not able often to know about them [breaches] because . . . they have scarce resources and as a result chances [are] . . . you can do it wrong and get away with it . . . . Now in the United States things are changing. Now the companies realize—and I would say that there is, and especially in some industries like financial insurance, there is a growing concern. As a result, there is a growing pressure on suppliers and all the companies around that supply services to them to be more demanding. I mean they are definitely more demanding in terms of security warranties.

iv. Increased External Engagement

External forces raising the publicity of privacy failures had the largest impact on DPOs at high-touch B-to-C companies. The increased publicity fed the activities of the consumer and labor organizations that were already focused on the firms. As a result, they developed a slightly more strategic portfolio, and, in particular, engaged regulators more proactively.

As one might imagine, providing legal advice and participating in auditing functions keep the Spanish DPOs generally highly internally focused. While all DPOs discussed interactions with regulators, the accounts varied widely across interviews. For most, interactions were relatively perfunctory and at arm's length. The DPOs reported the DPA as interacting with firms in three ways: "by specific inspection, from a complaint from a client or something like that, or from a specific review of one thing in the insurance market or Internet, e-commerce of insurance product." Importantly, the regulators, "don't call to you [and say] hey we are thinking about chang[ing] of the process." The DPA is viewed primarily as an enforcement agency: "DPA does not intervene in policies. They only act as police." The "DPA issues opinions . . . if you do not comply . . . and somebody tells them, you will be automatically fined."

But increased publicity has altered this pattern for high-touch business-to-consumer firms, as evidenced by their reports of more frequent interactions with regulators and other external players. This set of companies reported more proactive engagement with regulators, for example, about new products:

> For instance, you tell them "I am going to put this product in the market" and they say: "yes, no problem, come here and we will talk about it." Then you explain your situation to them regarding your product and they try to help you, they try to, because they are aware of the dichotomy of saying one thing but thinking something else.

These DPOs saw their value to the firm as partly derived from their ability to alter the relationship with the regulator. As one DPO explained, "we are working together with—not just with the—with the government. We are working together with []other governments about the privacy [and] international confidence. We share information . . . or ideas about the privacy."

These DPOs viewed proactive engagement as beneficial to their companies:

> [A]nother element could be the relationship with the data protection authorities [that is] good and friendly . . . . Because they are able to see the authority like a friend, not like an enemy and so sometimes we check with them [on] any matters without any problems, to help and so the people are more comfortable to ask different questions because they don't see a problem. They see a solution. It's a mix of the different elements . . . . The relation, the role of the authority, the innovation, different channels to sell their services, the pressure from the different administrations. It's a combination of different elements.

Another DPO, explaining why early meetings with regulators were of value said, "a big company like this one has to be really creative . . . in the beginning of new projects and everything."

The relationship between DPOs and the regulator was indicative of both the politically infused nature of privacy noted above and the relatively immature state of privacy professionalization coupled with little domestic history with self-regulation. While one DPO did report that the regulator contacts them proactively, primarily to use them as an example of best practices, no one reported being offered a participatory role in the governance process. The words of one DPO captured the sentiment of many: "Normally, they don't ask for the involvement of the entities. Normally, they . . . go their own way. They don't look to the sector for input. They make up their own mind and then impose it on the sector."

v. Increased Internal Authority

Increased publicity of privacy failures has also provided an impetus for internal improvements. For example, one interviewed DPO was actively developing a formal privacy infrastructure for an organization, which included pushing for hiring a data protection officer and establishing binding corporate rules for privacy. This interviewee explained the focus on those efforts by saying that, while the organization was taking care of privacy, "it's more operationally. It's not formally." The DPO thought that the formal title and structure was important for the company, and went on to explain that efforts to integrate privacy would "make them [employees] conscious of . . . [privacy] all over the corporation." This respondant also discussed efforts to use shared software and systems that support activities throughout the company and subsidiaries as a means to address privacy and confidentiality issues. Yet, while clearly taking a more strategic view about meeting compliance goals—organizing and simplifying corporate policies and practices and using it as an opportunity to educate employees about the meaning of privacy—the effort remained tightly oriented around the law. It was not used as an opportunity to discuss corporate values or principles, the way some of our German interviewees described. In an interesting juxtaposition, this DPO discussed using the adoption of binding corporate rules ("BCRs") as an opportunity to speak to the corporate leaders about privacy in an expansive way. This was done by tying the issue to their personal lives, linking it to various roles and experiences in society:

> And you try to tell them as people . . . [or] as an employee. That I would use your name and your daughter's name and your economic story and send it all over the world without control, without limit and to give [it to] my suppliers, my big ones for them to send you commercials? You don't like that? Okay, our customers don't, our employees don't, and . . . we have the obligation to maintain that in a correct standard. They say okay and they start to understand and they have influence . . . within the organization because if this is important for them, it will go down.

But, at the end of the day, although the DPO spoke of privacy internally as part of the relationship with various constituencies, the definition of privacy as operationalized in corporate practice retained its focus on the law. When asked about the content of the BCRs, that DPO said:

> Actually it's . . . binding corporate rules we have to follow very much like the standard of what the Spanish law established . . . . And taking into account that the Spanish [law has] . . . a very high level of requirements, I would say that if we comply with Spanish [law] we would be perfect as a group.

Following this compliance framework, the Spanish DPOs all reported using internal, and to some extent, external audits. Two of the four interviewed who reported auditing had begun to audit for privacy during the 1990s.

C. Privacy on the Ground in France

The French privacy leads interviewed portrayed a privacy landscape distinct in important ways from each of the other studied jurisdictions. More than privacy professionals in any of the other three countries, they articulated a historical understanding of privacy protection as synonymous with compliance and with concrete and specific requirements—largely regarding the registration of databases and their use, and the international transfer of data. This compliance function reflected, moreover, a largely settled understanding that one source defines privacy's meaning: the French data privacy authority, the Commission Nationale de L'informatique et des Libertés ("CNIL").[330] It also reflects an understanding that the general role of those responsible for corporate privacy is to comprehend, translate, and help firms fulfill the CNIL's mandates.

This understanding, and the singular role of the CNIL in defining privacy, is reflected in the operationalization of privacy within firms. Even in those firms we examined—those identified to us as leaders in the field—managers working on privacy were few in number and often spent less than full-time efforts on privacy issues. Many recounted their struggles in trying to focus attention on, and exercise influence in, integrating privacy mandates into firm decisionmaking, and, in particular, the challenge they faced in ensuring that their role was not simply relegated to raising data protection issues ex post, after resources had been committed to a project

[330] *See* Bignami, *Cooperative Legalism*, *supra* note 275, at 424–25 (explaining that CNIL's extensive regulations cover about eighty percent of all French data processing operations).

and actions had been undertaken. Moreover, they described privacy functions that were, in many cases, historically weak and limited, and, in most, highly centralized and siloed from other firm functions. Most strikingly, while each of the firms studied had sought to ensure, through their legal or compliance departments, that they fulfilled key requirements regarding registration and notification of data subjects regarding information use, in over one-third of the firms, the firm either had not created a single firm-wide privacy officer position until very recently, or still lacked such a position—although each was working on remedying that structural absence. Interestingly, a number of these firms had not yet even formally designated a data privacy officer, or *correspondant informatique et libertés* ("CIL"),[331] despite provisions under French law adopting, at least nominally, the DPO position, and offering certain administrative safe harbors should such a designation be made.[332]

The privacy landscape in French firms differed markedly from that of German firms, despite strong facial similarities in regulatory structure (the dedicated DPA/CNIL, and a designated DPO/CIL) and substance (a shared commitment to informational self-determination, and a social commitment to avoiding past abuses of data in Europe). French privacy operationalization also bore some resemblance to that of Spain, as firms in both countries approached privacy first and foremost as a matter of complying with regulator-determined requirements and therefore placed responsibility within the legal unit. Yet, while French DPOs faced struggles for influence similar to those articulated by their Spanish colleagues, their characteristics were far more diverse (they arose from operations and IT as frequently as they did from the legal setting), and the reasons they achieved reputations as field "leaders" were far more idiosyncratic. These differences often indicated far less about systemic aspects of privacy regulation, the privacy field, or the privacy dialogue in France, than about elements particular to the relevant firm, its industry, or the experience of either the particular privacy officer or of a high-level executive or board member.

If the French interviews painted a consistent portrait of the historically-low level of privacy's operationalization within firms and the idiosyncrasies of any efforts beyond mere compliance, they also reflected a nearly-uniform story of recent, and ongoing transformations in corporate privacy practices as the external privacy landscape that had gone largely

[331] *See Pourquoi Désigner un CIL?*, CNIL, http://www.cnil.fr/linstitution/missions/informer-conseiller/correspondants/pourquoi-designer-un-cil/ (last visited June 9, 2013).

[332] *See* Bignami, *Cooperative Legalism*, *supra* note 275, at 442–43.

unchanged since the early institutionalization of French privacy governance nearly forty years ago began to shift and recalibrate.

These transformations partially reflect new regulatory approaches. Notably, those interviewed frequently mentioned the importance of increased transparency and frequency of audits and enforcement actions brought by the CNIL, as well as a recent change in CNIL leadership. These developments signal changes in attitude regarding the challenges brought by changing technologies and resulting threat models, as well as alterations in the decisionmaking necessary to address them. Interviewees also noted that the CNIL's new emphasis on designating a CIL creates an entry point for regulators to more deeply influence the firm—although they recognized the shortcomings in the French regulatory definition of this DPO function, especially in comparison to its more robust German form.

Although they recognized that the development of the CIL has not alone sufficiently strengthened the internal corporate privacy function, the privacy leaders interviewed credited it with opening channels for a number of extra-regulatory influences to affect the firm's understanding of privacy. Specifically, it has facilitated exposure to best practices for robust privacy operationalization from other jurisdictions—including the United States and Germany—through professional networks that have developed in France and internationally. Though these connections have not supplanted existing French understandings of privacy, nor the importance of the CNIL in shaping norms, they have begun to expand the dialogue regarding privacy moving forward.

1. The French Understanding of Privacy's Meaning and the Limited Privacy Field

The French interviewees articulated, in the strongest terms, the social importance of privacy protection. They emphasized that strong privacy laws "protect the liberty of the people to have their private life," and are considered a "cultural" value arising "from very long history," and a "deep and specific sensitivity about privacy and data privacy." This sensitivity, they claim, arises from the experience of the *Shoah*—the Holocaust—and the use of data and databases in deportation and persecution during the Nazi period.[333]

This strong articulation of privacy's cultural importance and historic

[333] These articulations reflect official declarations regarding privacy regulation, as can be found in a recent influential report from the French Senate emphasizing the experience of the occupation as a ground for "extreme vigilance" regarding privacy protection. YVES DÉTRAIGNE & ANNE-MARIE ESCOFFIER, RAPPORT D'INFORMATION SÉNAT N. 441 (2009), *available at* http://www.senat.fr/rap/r08-441/r08-4411.pdf (Fr.)

roots, however, has historically translated into a rather specific understanding of how privacy must be protected: by focusing on individual rights and databases. The CNIL itself was created through France's early privacy law, enacted in 1978 (and amended in 2004)[334] in response to national outrage at an attempt by the French government to create a centralized database of personal data known as "SAFARI."[335] The CNIL's mission tracks this model. It focuses on keeping an inventory of data processing operations in both the private sector through a three level system of "notification" and approval—depending on the type and level of automation of the processing—to ensure that individual rights regarding that data, such as rights to access and inspection, are vindicated.[336] The agency is, in turn, vested with powers of advice and consultation to ensure that individual firms comply with these requirements and protect these rights. It also has the power to inspect and audit corporate practices and punish noncompliance with fines of up to €300,000.[337]

The interviewed privacy leads articulated an understanding of privacy protection as compliance with these CNIL-specific mandates. As one described, privacy is "mostly a legal question," and "[w]e don't have so much th[e] kind of situation in France" in which corporate behavior is legal, but people object "because the law is normally . . . kind of strong." Indeed, another explained, that the CNIL tries to leave little flexibility as to the rules regarding data processing and rights protection, producing "very detailed and exhaustive checklist[s] of what you need to do in order to be compliant." As a third described:

> It's not principles that they put there. It's for a given purpose in a given situation you have to [do this or] that . . . it goes to the details, you have to put these sentences [in] a consent form. You have to give access only to the people who do accounting and not to the people who do reporting and it's really going to be more detailed.

[334] *See* Loi 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1)[Law 2004-801 of August 6, 2004 regarding the Protection of Individuals Regarding their Personal Data and modifying Law 78-17 relating to Data Processing ,Files, and Freedoms], Aug. 7, 2004 (hereinafter 1978 French Law, as amended).

[335] *See* Phillipe Boucher, «*SAFARI*» *ou la Chasse aux Français*, LE MONDE, Mar. 21, 1974.

[336] *See* 1978 French Law, as amended, arts. 22–24; *Missions and Powers*, CNIL, http://www.cnil.fr/?id=630 (last visited June 9, 2013).

[337] *Independent Administrative Authority*, CNIL, http://www.cnil.fr/english/the-cnil/its-operation/ (last visited June 9, 2013); *Missions and Powers*, *supra* note 336.

In the words of a fourth interviewee, discussing requirements regarding the format of stored data:

> The CNIL would like to give precise instructions . . . for example, when there's an authorization, they'd like to list the type of data one by one. You're allowed to use the last name, the first name, gender. This is very difficult for us, because we have a lot of data. So we prefer that the CNIL give categories of data. Data of identification, instead of listing it one by one, because they'll be missing some. And if they're missing some, we're not in accordance with what they said. We want them to stay within concrete principles, but not too detailed, because then there's always a discrepancy, and that's not progressive.

As a fifth privacy leader we interviewed describes, "[t]here is a risk that the CNIL [will] be too specific" in an unnecessary manner, so firms "will not be in a position to do [their] . . . day-to-day work." "In the end," however, as another privacy lead describes, "it's the CNIL that decides."

The CNIL, which has the largest number of employees of any data protection authority in the jurisdictions researched, is structured to provide detailed guidance not just in categories of similar cases—for which they have also developed "simplified" notification procedures—but also as individual questions arise within firms. Interviewed privacy leads described this consultation as frequent, ranging from monthly to yearly. "[O]ften, when I have a case [that's] a little complicated," explained one privacy officer, "where I'm not sure I'll have the authorization of the CNIL, I go see them . . . to have their recommendation. This has, honestly, always gone very well." "This company wanted to create this treatment of data, it went to [me as] the CIL," described another lead of a recent experience,continuing:

> Based on the data we're collecting, we may have to get an authorization from the CNIL. So we set up a meeting at the CNIL, we explained what we wanted to do, they told us, this is okay, this isn't. So the [firm] integrated in the contract what needed to be done, and today, the contract works.

Many of our interviewees also mentioned CNIL workshops and conferences, during which they explain appropriate ways to handle particular recurring situations, as well as guidance published on the CNIL website.

As many of our interviewees explained, these modes of communication have been further streamlined by creation of the CIL position in the 2004 amendments to French Privacy Law.[338] The CIL is a data privacy "correspondent" position that firms can voluntarily designate to both assist the organization with respect to Data Privacy Act compliance, and to serve as a means of communication between the firm and the CNIL.[339] The appointment of the CIL provides certain compliance advantages to corporations, as it exempts them from many CNIL notification processes, and places the duty of ascertaining compliance on the designated agent within the firm.[340] It also facilitates the conveyance of administrative advice and guidance into the firm, through the creation of a designated office within the CNIL for CIL communication, and with resources such as an extranet site dedicated to these DPOs, which offers "a platform for preferential exchanges, fora, Q&As, form specimens, and training material prepared by CNIL departments."[341] As one respondent described, "the CNIL put in place a unit dedicated to interfacing with CILs. So when we have a question to ask the CNIL, as a CIL, instead of going through an administrative process, we have privileged answers, with a quick turn-around time."

The CNIL's role as the source of detailed rules regarding privacy's meaning in particular implementations, moreover, contrasts with the negotiations about privacy's meaning in other jurisdictions. The dialogue over privacy in the United States involved a variety of parties including advocates and regulated parties as well as the FTC,[342] Germany's privacy "field" includes robust roles for workers' councils and strong DPOs within the firm,[343] and Spain's landscape incorporates labor unions and consumer groups in shaping the meaning of compliance.[344] Such nongovernmental forces, however, are largely absent in the accounts of French privacy regulation. Our interviewees explicitly rejected the importance of "advocacy groups," "consumer organizations," and "labor unions"[345] in the dialogue over privacy's meaning. One did suggest however, that the involvement of workers might be changing, describing how unions "do ask more and more for information that concerns them. And this is very new.

338 *See* Loi 2004-801.

339 *See Pourquoi Désigner un CIL?*, *supra* note 331.

340 *See id.*

341 *See id.*; CNIL, 30E RAPPORT D'ACTIVITÉ 7 (2009), *available at* http://www.cnil.fr/fileadmin/documents/en/CNIL-30e_rapport_2009-EN.pdf.

342 *See supra* note 212 and accompanying text.

343 *See supra* Part IV.A.1, 2.a–b.

344 *See supra* Part IV.B.1.

345 Responses included: "there's not this sort of issue;" "the advocacy groups have been quiet;" "in France, this isn't a subject that is handled by consumer associations;" "it's not a tool that unions will use a lot."

That's because the press talks a lot about this subject. So the unions are starting to ask us a lot of these questions."

One interviewee directly attributed the contrast between the French and German workers' role in the privacy dialogue to specific legal differences in the structure of the workers' councils. While such institutions exist in both countries that privacy officer explained:

> [T]hey . . . only they have limited rights [in France], much more limited than in Germany. In Germany you have to remember the board of director[s] of German companies is made half a representative of the employee[s], half a representative of the shareholders which means that they have a very strong weight . . . . [S]o basically when a company wants to do a major reorganization, sell part of the company or buy part of the company, they have to be involved, the workers. In France they don't. They have to inform people of this change but they don't have to follow their opinion. In Germany works councils can decide, they can block the use of [a] system or block a process in the company.

Our interviewees made a similar distinction between the structure of the German DPO, and the French CIL. While both are designated pursuant to law, many of our interviewees described the French version of the position as far less influential because it lacks the job-protection provisions accorded to its German counterpart. It also lacks the same sense of independence in feeling free to report noncompliance.[346] Those interviewed did, however, as discussed below, credit the CIL position with increasing access within the firm to the corporate board, and thereby enhancing attention to privacy as a subject.

As one respondent described, "[t]hey are not so protected [as they are] in Germany, so I do not see a CIL calling the CNIL to alert about misconduct." In the words of another, "it's not in our culture to go denounce our company. I don't know how we'll handle this." One European lawyer, contrasting their experiences in a number of jurisdictions, explained:

> There is a specific dedicated department from the CNIL to help the CIL, but the CIL is very cautious because the CIL wants to avoid audits from the CNIL. So if you say too much to the CNIL, it'll be interested either to better understand the industry, or to know more, so they are cautious with the CNIL.

[346] *See supra* notes 292–293 and accompanying text.

Summing up the importance of this distinction, one French CPO specifically connected it to the multifaceted network of privacy governance in Germany and the increased government role in France. "Frankly when I try to think," the CPO summarized, "they don't do a lot of inspection in Germany. Because they have the DPO basically report to them all the time so they have people in-house."

Finally, our interviewed privacy leads explained that, despite the opportunities for communication with the regulator, regulated firms played little role in shaping policy (except for a recent trend towards input by professional groups discussed below). "[I]t's more when we're working on concrete cases," said one, "it's not at the point where we're discussing the doctrine with them." "I think in the future, it maybe something we are interest[ed] in," said another, "[b]ut for the moment, now we are [focused on] our day-to-day business."

2. Operationalizing Privacy Within the French Firm

In some ways, the privacy officers differed in their opinions on the effects of a governance model centered on the regulator's detailed requirements. One explained that such rules provided the sense that "we have the means to be in conformity . . . [so] we don't consider it to be one of our top five risks." Others focused on the fact that regulations, at this level of specificity, are "extremely cumbersome," and that such rules "require a lot of things," explaining—like their Spanish counterparts—that a focus on such top-down rules makes it "completely impossible to be 100% compliant."

But in every case, the interviewed privacy leads described consistent effects in terms of the way their firms have approached privacy, and its implementation. Most notably, their accounts reflected the ways in which this model of governance has traditionally led to the allocation of privacy efforts to lower-level lawyers, or to compliance units reporting to the general counsel, which those interviewed articulated as the natural site for responding to the CNIL's notification mandates.

Yet because our study focused on privacy professionals identified as "leaders," our interviewees described ways in which they rose to positions of privacy responsibility unusual in the French context, describing an additional governance layer on top of their legal compliance function. Their backgrounds were diverse. As one interviewee accurately described the group of French privacy leaders, "[w]e say that there are three types . . . . There's the more technical profile, there's the more judicial profile, and there's the conformity/audit profile." And the ways in which their firms came to the decision to develop a designated privacy function, and the resources that go along with it, was also far more varied than the stories of privacy officers in other jurisdictions.

For two interviewees, a single board member in each of their firms recognized the growing importance of privacy, and made the case for the allocation of additional resources. In one of those two firms, that board member went so far as to try to use privacy leadership as a market differentiator. Other privacy leads already held positions within the firm—for example, in information security or audit—that commanded significant resources or a direct board report, both of which benefitted privacy when that subject was added to the executive's portfolio. Some worked at firms in industries that dealt with sensitive information and were governed by other relevant legal frameworks through which the eventual privacy officer developed expertise in information management compliance. In still other cases, advances arose when privacy was integrated into the consideration of preexisting, robust, and unrelated risk-management systems—such as information security—or a well-developed "code of ethics," or other information management and audit systems. As one interviewee working in an otherwise highly-regulated industry described:

> If, let's say if privacy aspect[s] were not considered originally, and very often they were not, it is easier to just add a few provision[s] in the existing methodology; it's the best way to ensure that the system that will deploy will have been assessed for privacy and data protection and that the people will follow the rule in practice.

In the words of another with an information-security background, by adding privacy into security frameworks governing the approval of new IT systems, "I can just push my different ideas inside so we could be able to do some 'privacy by design' more easily than if we did not have a formal process already in place." And in the case of a third privacy officer:

> [P]rivacy is part of the whole package, so we have an ethics code, and privacy is part of it but it's much larger than that so that means that you fight corruption, illegal interests, conflict of interests, you fight [corruption] and [it] is more or less the same and then you promote equal rights from women or minorities and so on, so this is the whole package and within this package you have also privacy and personal data protection.

Despite individual accomplishments in piggybacking privacy onto other, better-developed firm functions or positions, the size and general privacy focus described by most of our interviewees diverged sharply from those of their German and U.S. counterparts. With the exception of one

CPO who coordinated the efforts of designated CILs in multiple subsidiaries within France, few French privacy leads described an operation within their French firm that involved more than one or two professionals working full-time on privacy. More than half of the identified privacy leaders we interviewed, moreover, were not dedicated to the issue full-time. Some spent as little as fifteen or twenty percent of their time on privacy. Most were the first privacy officers in their firms, and most received their privacy duties within the past four years.

A number described the steep hill they have had to climb in making the case for a stand-alone privacy officer in their firms. One of the longer-serving privacy officers described the experience of initiating a privacy function a number of years ago: "You have no clients and you have no boss, you know. And you are alone in the desert . . . . And you are just alone. Nobody cares, nobody wants [it], it's a burden to everybody." Another described: "When I started my job . . . we ha[d] many projects which [raised privacy issues] and it was a difficult time because I had to say 'no'. 'No, it's not possible.'" And a third stated, "sometimes it's very difficult [in] meetings, because I say, 'this, we're not going to do.'" Even those at the more fully-resourced end of this narrow spectrum headed a centralized privacy operation that was generally not well integrated operationally within the firm. While a few described the designation of a privacy "correspondent," or interlocutor, within diverse business units, none described the embedding of dedicated privacy experts.

For many, their privacy work focused on education efforts about the importance of privacy, attempts to increase awareness of privacy mandates, and, especially, the translation of legal requirements regarding data processing through training—in person and online—and written materials for firm workers. As one CPO described:

> [W]e gave a lot of presentations to train people on the protection of data. We prepared presentations in the form of questions. We put together pamphlets to raise awareness on the important points of the law. I wrote procedures to explain to people how to analyze whether their handling of data conforms [to the law].

Another privacy lead described the way in which privacy officers develop policies governing data for other firm units:

> At first we come up with points that we think are important to develop internally, it can be the right of access, the requests of third parties, because we are very much solicited, not necessarily by clients, to obtain information about our employees . . . . They come to see us asking for information on so-and-so . . . . So we

> had to teach our colleagues how to respond to this sort of request. Also, how to react when we have a request for a right to access a person's personal data. We had the will to develop a framework for this. So we develop the idea, we prepare a notice, and after we have it validated by either marketing to have it placed on our website, a tool for the candidates to explain to them how they can access their data, or a notice that is worked in collaboration with the legal team to be published in our legal reference on the requests of third parties and how to respond in these sorts of cases, and makes reference to our existence.

As a third privacy lead described their duties:

> [W]e give the law. And then we say . . . here's what you have to do, what we must not to, what's not allowed. And if you do it wrong, here are the sanctions. We explain to people how to work, while respecting the law. So that's the first thing, we make guides. We made some for HR, we made some for everything that is archive[ed] . . . . So we made a guide for each type of work, saying for each type of data, how much time you must keep them. The law says this, and we, CIL, recommend this.

Others explained that building personal relationships with the leads of other units such as marketing and IT makes them institutionally well-placed to guarantee consultation as new projects and technology systems are rolled out. "[S]lowly and slowly," one explained, "that's mainly my job. Teaching, making rules, convincing, making bridges all over." This was ensured in some instances not just informally, but by company policy: "I'm involved at the beginning of [every project that comes from the central part of the company]," explained one CPO. "It's in the technological procedures. In projects, before passing the first step, they must come see me so that I can tell them, here's everything that needs to get done."

As discussed below, at least three of those interviewed—all in firms who had recently developed or revamped their privacy functions, and all of whom came from either core firm operations or IT—had developed a CPO profile that more closely resembled that described by their German counterparts in a variety of ways, suggesting a new model of privacy lead among the diverse mix of the French experience. They appeared especially integrated into core firm decisionmaking both by their intimate knowledge of the personnel and their relevant functions. In two cases, the privacy lead served on a high-level trans-substantive corporate committee developed for the purpose of integrating a variety of firm interests into firm project planning.

At the same time, most of the privacy leads—including the abovementioned three—described a largely-centralized approach to developing privacy policies in these consultative contexts. In describing this orientation, and the decision not to develop a privacy expert within different departments, one explained:

> [T]he goal of the game is to discuss this with all of our colleagues. The idea behind our system is for each individual to have the right reflex. As a result of discussing with everyone, it sets the right reflex, and the next time, they'll come consult with us out of their own reflex. So no, there's no point of contact in the marketing department.

In the words of another, "we prepare [our policies] by ourselves, our team. And after, we solicit experts, we ask them questions. But in general, we have the knowledge to make the guides, so we don't have too many issues. Then we distribute them."

Even those two CPOs, however, recognized that such centralization is both "an advantage and an inconvenience." As one explained, "[t]here's a risk of missing something. But from our end, since we have the expertise, it's more interesting and constructive to have the marketing expert to explain to us their problem, and we'll work with them to go in the right direction, as opposed to diluting." The second privacy lead stated:

> We diffuse within the enterprise that when there is something new, they must alert me . . . . For the big projects that are expensive, I am aware, because it's something that is important in the enterprise, and for that, I'll oversee what is implemented technologically, and say, this is possible, this isn't possible. But for cases that are less important, that can be serious if they're not well done, but that are less costly, I'm sure there are some enterprises where things are done, and I am not aware of them.

3. *Suggestions of Transition in the French Privacy Field*

The French interviews showcased the generally low level of privacy operationalization within firms and the shortcomings of efforts beyond compliance in firms with privacy leaders. They also revealed a story of a privacy landscape that—although it had been largely unchanged since the comparatively-early institutionalization of French privacy governance nearly forty years ago—was in the midst of a recently-begun transformation which was affecting corporate privacy practices.

a. Shifts in Regulatory Tools and Approaches

These transformations partially reflect a shift in regulatory tools and approaches utilized by the CNIL. Indeed, while the interviewed privacy leads noted that the agency's practices may, in the past, have reflected an evolution of existing practices such as the adoption of simplified notification policies for standard uses of data—they attributed more revolutionary change in the privacy landscape to several recent shifts in approach.

The first involves an increase in both the frequency and transparency of inspections and enforcement actions. As one CPO explained, by reducing the administrative burdens of notifications, the CNIL has:

> [R]eplace[d] it by commitment to follow a certain methodology or apply a certain simplified rule . . . . This allows them to free up resources to do more inspections . . . . In the past you had to notify or ask for the authorization for everything which of course is a huge [amount of] paperwork for very little . . . benefit . . . [a]nd they were dealing with paper mountains accumulating in their offices.

Now, that privacy lead explained, "they have an approach which is . . . closer to the Anglo-Saxon way of doing these things: This is a rule. That's what you have to comply with. You don't have to notify but we will come and check. And they are doing that more and more."

Indeed, every respondent we interviewed mentioned the attention brought to bear on privacy actions by the increase in the CNIL's surprise inspections and audits, which the agency indicated grew by fifty percent in 2012. Moreover, these actions, and any sanctions to which they lead, moreover, can now be publicized,[347] after passage of an amendment to French Privacy Law, the "Defender of Rights" Act, passed on March 29, 2011.[348]

In particular, our interviewees noted the importance of the agency's articulation of its upcoming audit foci in grabbing people's attention and focusing firm priorities. Indeed, sixty percent of the firms studied reported having been the subject of a CNIL inspection in the last several years. The practice of publishing the audits, and their results, was noted as particularly

[347] *See The Sanctions Imposed by the CNIL*, CNIL, http://www.cnil.fr/la-cnil/missions/sanctionner/les-sanctions-prononcees-par-la-cnil/#c4709 (last visited June 9, 2013).

[348] Loi 2011-334 du 29 mars 2011 relative au Défenseur des droits [Law 2011-334 of March 29, 2011 relative to the Defense of Rights], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Mar. 29, 2011, art. 8.

important in this process. In the words of one CPO whose audit was "pretty positive," the audit marked "a success that we could transmit to our CEO, to tell him that it went well, that we got remarks, but also compliments on our tools." Another reported that after an audit, the company decided to elevate a privacy professional within the firm to the position of CIL.

The interviewed privacy leads credited the rise in enforcement actions with increasing firms' attention to the issue of privacy, and for the development of a notion that privacy failures can lead to real reputational risk. Several privacy professionals mentioned, in particular, the effect of the CNIL's 2010 ruling against the private tutoring firm Acadomia, a decision posted publicly[349] and widely covered in the press,[350] as a turning point. One explained: "This played a large role [in] the awareness of organizations on the risk of reputation related to IT law. We also played a role, because it allowed us to bring awareness to our teams of the risks that can result if there's a negative audit of the CNIL." A second agreed, stating:

> [T]here was this reputation risk that was identified, and so I talked to the CEO about it, who said, "[o]kay, let's put together the means to remove this risk." That . . . [meant] an investment in information technology to add popups in the comment fields, investments to do automatic audits. There was a decision made, let's make an investment to deal with this.

Another described the importance of informing the firm's board about the public sanction of a French bank, which involved "a fine plus [a] specific article in the news," as well as about "other examples for other companies, and . . . show[ing them] . . . that [the] CNIL was doing [inspections] inside our own company." A third spoke of systemic enlistment of this type of publicity to generate support for recent changes within the firm. As the lead described:

> It helps me. So, more and more, there are scandals that are revealed by the media. So that helps me to pass the message internally that this is a real subject. Every month, I send out a press review to all the big bosses, with decisions made world-wide, from the . . . [United States], from England, with big

[349] CNIL, DELIBERATION NO. 2010-113 OF 22 APRIL 2010 CONCERNING THE RESTRICTED WARNING AGAINST SOCIETY AIS 2 ACADOMIA, *available at* http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/230/.

[350] *See, e.g.*, *Acadomia Epinglée par la CNIL*, 20MINUTES.FR, May 27, 2010, http://www.20minutes.fr/societe/407540-acadomia-epinglee-cnil.

> scandals, to try to make them aware . . . . Yes, there are some who have told me that it's starting to interest them. But it's recent.

In the words of a fourth interviewee:

> [R]eputation is important for the company. We have shown that other French companies, banks and other types of companies had specific controls from the CNIL regulator and they had either penalties to pay or they had to write specific articles in the newspapers and so in terms of image it's not a good thing.

While several privacy leads suggested that the CNIL needed to increase their actions even further in order to increase public pressure, they generally recognized that CNIL's expanded enforcement actions have already affected the public's awareness. For example, while one said, "I think it's not enough," another warned, in light of the CNIL's new decisions, "we have to be sensitive to what we call in France 'l'opinion publique,' public opinion."

The second regulatory development cited by interviewed CPOs reflects several changes in the CNIL's approach to thinking about privacy as a result of new leadership. Several cited public remarks by the new CNIL President, Madame Isabelle Falque-Pierrotin, as indicating that the CNIL intends to use more and more ex ante guidance, to rely less on formalities, and to credit firms for developing robust privacy systems, even when breaches occur inadvertently. In the words of one CPO, "I had the feeling that we were at a major turning point in France. And that we were in the middle of going from this approach of nonconformity to an approach of the management of risk."

Other interviewees mentioned two other CNIL changes that have led to shifts in the privacy field: the integration of a team of technologists into the CNIL's staff; and, the development of a new CNIL Department of Innovation, which is managed by the agency's former general counsel, Madame Sophie Vulliet-Tavernier. One privacy lawyer we interviewed described how these new units function:

> There is a team dedicated to innovation, which works with academics, sociologists, engineers. They have a big meeting on innovation. There's one department dedicated to technology, with engineers, who will work on the new regulation. But there is also a new department dedicated to prospective innovation. And they work with all types of stakeholders dealing with innovation.

"It's really very open," that privacy leader continued, "[i]t's no longer just lawyers and IT providers, it's all types of people who think about the evolution of privacy [including] consumer associations [and] representatives of the education industry." According to our interviewees these developments, moreover, reflect a broader change: a greater level of overall flexibility in those responsible for coordinating privacy compliance in arenas. As one CPO described:

> The people of the IT department are very business oriented, very open minded, but the civil servants who are working on the day-to-day notification, they are less open, they are more strict. So when you want the CNIL to evolve or be more business oriented, you need to escalate past the first level. The top level is more business oriented than the people who handle the day-to-day.

A number of interviewees cite the new CNIL department as providing new opportunities for stakeholder involvement, including discussions about policy between the CNIL and outside groups representing specific data-intensive industries like health care, banking and insurance, and privacy professional groups. A number of our respondents commented on this trend, explaining:

> [That] the professional organizations are more efficient in discussions with the CNIL . . . [and] that the CNIL prefers to collaborate with professionals when it's working on a specific subject. It'll discuss with banking organizations when it's on a banking subject, and it'll discuss with health professional organizations when it's working on health data, but I think that it prefers this because it has people who know what they're doing.

In particular, at least one lawyer explained that, while companies might not feel comfortable "lobbying" the CNIL themselves, given their position as a regulated party, these industry groups might now be able to present important perspectives in a more secure manner. When I "intervene in the regulatory lobbying" through a professional or industry organization, explained one CPO, "it's not as a representative of [my firm], it's as a professional [so] it's a little different." Describing the work of the French privacy professionals' organization, another phrased the issue more strongly: "from time to time, we work on certain subjects where we'd like to remain anonymous. So the work group arrives at a conclusion. And it's this group with only anonymous people, in other words, under the cover of the association that goes to present the case to the CNIL."

b. Maturation of the CIL Position

A number of interviewees suggested that the maturation of the position of the CIL is an important, albeit recent, development. To be sure, the CIL position has officially been on the books for a number of years. Yet the comments of some privacy leads, especially those who have taken on a formal privacy lead position recently, suggest that the recent development of a more formal CIL position is a useful focusing point for generating both a more influential privacy professional presence, and a more robust internal privacy practice.

Although those designated as CILs earlier in the position's lifecycle appreciated the streamlined regulator access and administrative procedures it provided the compliance function, they spoke less about the position's capacity for heightening influence and independence within the firm. But the accounts of several more recent CILs suggest a strengthening CIL role in France. Sounding very much like a counterpart in Germany might, one CIL designated as such over the past year described confidently, "I'm independent, by the law. The French law says that when a CIL is appointed, he is independent. That means, that it's written in the law, that no one should tell me what to do, nor how to do it." Key to that independence, in that privacy lead's view, was access to the corporate board: "[R]eporting to the CEO is in the law" as is the duty to alert:

> If there's a functional problem in the company, for example, data that was accessed by people who shouldn't have, and I'm aware of it, and my colleagues did not do as they were supposed to, I must alert. So I have a procedure that I put in place, where I notify the alert. First to the director who should know in the enterprise, pretty high up in the enterprise, to tell them, here is the problem, here is the law. What will you do to correct this? When will you correct this?" [And] when I do an alert, I do two or three per year, it's corrected in the month that follows.

Several other interviewees described the designation of a CIL as an organizing event in their companies involving a complete reworking of the privacy function, with new structures, resources and attempts to enhance the privacy lead's legitimacy and involvement in firm decisionmaking. More specifically, two CILs spoke of the way in which the formalization of their title and role involved their placement on "transversal" committees—either ongoing, or assembled as new projects arose—that handled development from a corporate project's nascency, and therefore ensured that privacy requirements would be articulated, and guidance given, throughout a project's lifecycle.

Finally, the rise of CIL designations coincides with the development over the past few years of institutions to support privacy professionalization in France, discussed below. Professional networks can now provide support, guidance, organization, and information about best practices that can shape the views of designated internal corporate privacy leads. As one brand new CIL understood the elements of a cutting-edge privacy practice, by integrating privacy into existing technology systems, his firm would "do privacy by design and implement in this process . . . specific items for [a] privacy impact analysis." When asked from where this notion of privacy derived, the CPO responded, "[i]t's because I've attended the IAPP conference in Brussels and I've heard a lot of it and I . . . [saw that] it would be coming in the next regulation."

c. Privacy Professionalization and Best Practices Influences

This last quote points to the recent development of an important role for privacy professional organizations generally, identified by every privacy lead interviewed as now becoming "important players in the dialogue about privacy." Together, the interviewees gave an account of the robust role that such overlapping organizations—in particular the French Association Française des Correspondants à la protection des Données à caractère Personnel ("AFCDP") and the U.S.-based IAPP—are coming to play in evolving understandings of corporate data privacy. As one interviewee described, participation in these groups:

> [B]rings us to the forefront, to the new topics. It allows us to meet colleagues. Because if one day we have a problem regarding health, we can contact the CIL of a hospital. Since we have clients with various jobs, it creates a network of diverse expertise. We really have to spend time externally to acquaint ourselves with the news.

It also creates a network to "get information first," about how new technological issues "ha[ve] to be conceived of," and the "legal obligation we have in this respect." And, in the words of one active participant, "we define best practices."

Privacy leads explained that such information is disseminated through association websites, conferences, lunches, webinars hosted on association extranets, work groups, online discussions, "knowledgenet" events, and lunches at law firms. The existence of a professional network, along with international conferences such as the IAPP summits on both sides of the Atlantic, and the annual Privacy Laws and Business gathering in Cambridge England,[351] bring models from a variety of countries across jurisdictions. "I'm attending a conference on next Monday to get more information on the situation and I've talked also to some people from . . . the [United States] who worked on this," said one interviewee. Another

[351] *Annual Conference*, PRIVACY L. & BUS., http://www.privacylaws.com/annual_conference/ (last visited June 9, 2013).

stated, "we've been inspired by what's going on in the [United States]" (adding, "[b]ut simply, we don't have the same culture."). "[F]or me it's great," explained one new privacy lead, "because I[] enlisted in the IAPP last October to attend the conference and to be in the network of privacy professionals on the international side." Indeed, that CPO explained, "I will get with the IAPP I guess all the feedback I would need to implement my activities and defend inside the company some good practice to implement." In short, explained another, "to be a good CIL, you have to be a part of an association."

V. Preliminary Lessons from The European Research

This initial review of our empirical data regarding corporate privacy management in Germany, Spain, and France, and its comparison with similar interview responses from the United States, suggests important insights for regulators crafting privacy reforms, corporations that will be bound by new regulations, and civil society organizations seeking to ensure their efficacy. To be sure, our research is not structured independently to analyze how well privacy is protected in any given company or jurisdiction. But it provides a basis on which to consider and compare key issues that should inform regulatory reform, including how thoroughly firms in various jurisdictions attempt to ensure that the prevailing understanding of privacy pervades corporate decisionmaking and practice; and what aspects of the privacy field—regulatory and other—contribute to corporate choices that promote the sustained and thorough attention to privacy that scholarship suggests leads firms to more firmly embrace, and protect, external values.

Our collected accounts indicate fundamental shortcomings in the existing narratives regarding U.S. and "European" privacy law, which portray binary approaches diverging on measures of commitment, comprehensiveness, and coherence.[352] Our inquiry reveals similarities and differences between jurisdictions along a variety of dimensions that a singular focus on privacy on the books obscures. Our inquiry further reveals shortcomings in the limited prior scholarship that did go beyond formal law to consider dimensions of regulatory process—institutions, procedures,[353] and instruments—showing that it too fails to capture salient aspects of the overall external environment that influence privacy's protection.

Fundamentally, our inquiry suggests that (1) accounting for how, and

[352] *See supra* note 65 and accompanying text.

[353] *See supra* notes 74–83 and accompanying text.

how well, corporations adhere to the privacy commitments articulated in formal legal frameworks depends upon a complex set of factors outside those frameworks, and (2) different permutations of those factors can produce similarly promising, or similarly disappointing, results. To put it another way, jurisdictions with facially similar regulations can produce very different sets of corporate privacy practices, while facially different national regulatory frameworks can spur privacy decisionmaking structures within firms that are strikingly similar.

Specifically, our research indicates that the way privacy protection is actually understood and operationalized in corporations is shaped by a disparate set of public and private actors, practices, and institutions producing constraints at times more powerful than those created by "black letter" law and formal legal institutions.[354] We do not claim that formal regulations and institutions cannot drive corporate behavior toward more privacy protective policies and practices. Rather the claim is that, in the face of rapidly changing technologies and business models—and the resulting challenges for privacy protection—they will do so more effectively if they catalyze the construction of a social license that triggers the sort of regularized feedback loops and decentralized structures of modeling and control that leads individuals and firms to internalize external values as their own.

A comparison of the four cases we examined indicates that there are a set of regulatory choices that can combine to spur (or not) these more adaptive responses. This set includes choices about the specificity of regulatory mandates (such as between rules and standards), the modalities of regulation (whether they are closed and unilateral as opposed to open and consultative), and regulatory transparency (whether regulatory efforts are episodic, attention-generating, and geared to promote interaction with constituencies, as opposed to regular, bureaucratic, and behind-the-scenes). In particular, these choices affect whether regulatory practice fuels a multi-stakeholder privacy field, and whether notions of privacy are nested within broader ethical frameworks that can harness other political, marketplace, and workplace forces against an impulse towards reducing privacy to bureaucratized and simplified practices within the firm. Where this can occur, this field of external actors—regulators, advocates, workers, and importantly peers—can develop the sense of a need for deep privacy expertise within firms. That expertise is required to embed privacy, in all

[354] Bradley Karkkainen explains how this works in the field of environmental regulation. Bradley Karkkainen et al., *After Backyard Environmentalism: Toward a Performance-Based Regime of Environmental Regulation*, 44 AM. BEHAV. SCIENTIST 692 (2000).

its ambiguity and richness, into business and operations—including technical design.

Understanding, then, in a granular fashion, the experiences of a number of different jurisdictions in regulating privacy to date, provides insight into several key aspects of privacy reform under consideration in ongoing global debates. For such an understanding begins to illuminate the question of which legal standards, as well as administrative structures and modalities, in combination with which social contexts, both enable regulators to evolve and adapt protections to address privacy threats wrought by rapid technological and business-model change, and to promote corporate structures that weave privacy into the daily life of the firm.

While we will ultimately present a comprehensive account of the varied lessons for privacy regulation that ought be learned from the detailed comparison of jurisdictional divergence,[355] at this initial stage of analysis, we will sketch out early hypotheses related to two sets of issues that impact these questions of regulatory adaptivity and firm responsiveness. These two issues are: (1) the way different choices about privacy's institutionalization affect the extent to which privacy is viewed either as a dynamic social constraint on firm behavior—infusing all aspects of corporate life—or a regulatory obligation farmed out to the compliance department or outside counsel; and (2) the importance of privacy professional networks in the diffusion of dynamic responses to changing privacy challenges across jurisdictional lines.

Our findings regarding privacy's operationalization in firms in these four countries have important implications for current debates about regulation, including the proposed E.U. data protection regulation.[356] They offer critical data to inform policy debates over both the substantive meaning of privacy and the form of its regulation, with particular import for understanding the ways in which the latter catalyzes corporate privacy practices in the face of technological advances and the new challenges they portend.

A. Operationalizing Privacy: Identifying Key Practices for the Adaptive Protection of Privacy

The countries studied all undertook regulation premised on an understanding of privacy's meaning that was adopted thirty years ago:

355 BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 13.

356 *See* Press Release, European Commission, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012), *available at* http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

privacy as informational self-determination, and FIPPs as the mechanism of protection. Yet they diverged sharply on choices about the regulatory process—the institutions, procedures, and instruments of protection. Additional factors, such as the general legal culture, traditions around advocacy, and market organization were similarly distinct and, as we discuss below, play important, yet previously underexamined, roles in regulating corporate management of privacy. Even within Europe, where a shared directive constrains variance, decisions about the selection and positioning of privacy regulators, the hard and soft powers they wield, the sources of economic support, the position in the political and policymaking landscape, and their connections to other sources of authority and power, vary tremendously. These decisions have profound implications for whether corporate behavior can be tempered to protect privacy adaptively in response to new threats.

Perhaps the most striking result of our on-the-ground research was what it revealed about the ways in which corporations in the four studied jurisdictions arrayed along an axis measuring the extent to which corporate behavior and structure reflected a commitment to integrating privacy into firm decisionmaking, organization, and culture. Germany and the United States clustered along one end of the spectrum, demonstrating important similarities in internal practice involving the level of the privacy function within the firms (high), and that function's broad integration—both through personnel responsible for privacy, and technologies and processes geared to raising and incorporating privacy concerns—throughout decision structures in varied business and product lines. In contrast, the relegation of privacy expertise to centralized, generally legal, staff dominant in Spanish firms, the inconsistent level of attention and structure accorded to the privacy function in French firms, and the focus in both nations' firms on compliance with specific formal reporting requirements, suggests apparatuses ill equipped to weave privacy into businesses or deliver the sort of early interventions that go beyond "the margins."[357]

More specifically, the on-the-ground account of privacy describes the emergence of a suite of best practices in leading U.S. and German corporations. These include: a high level of attention, resources, and prominence for the privacy function within the firm; the integration of privacy decisionmaking into technology design and business-line processes through the distribution of privacy expertise within business units and

[357] *See* Nigel Waters, *Privacy Impact Assessment—Great Potential Not Often Realized*, *in* PRIVACY IMPACT ASSESSMENT 149, 150–51 (Wright & De Hert eds. 2012) (explaining that privacy must be built into new systems rather than added to existing systems where the "parameters have been set").

assignment of specialized privacy staff to data-intensive processes and systems; and a high-status privacy lead who mediates between external privacy demands and internal corporate privacy practices. These practices resonate with both recent scholarship and policy advocacy regarding both the broadening of the substantive understanding of privacy values that must be protected, as well as the related importance of incorporating privacy "by design" into corporate structure.[358] These, in turn, reflect the scholarship of organizational theorists more generally regarding the optimal manner of incorporating secondary interests that may be in tension with core firm goals—such as the institutionalization of privacy protection, into corporate decisionmaking.[359]

1. *The Promise of Privacy "Managerialization"*

In particular, these practices mirror recent suggestions that, to be successful, privacy must be moved outside the legal domain and into that of technology design and business processes.[360] By contrast, envisioning privacy as it has been traditionally understood—as a legal exercise—limits it to legal compliance's traditional function as a post hoc intervention, "undertaken well after the main design parameters have been set, an organisational structure committed, and significant costs incurred."[361] Understanding privacy in that way limits the integration of privacy values:

> Clients will rarely welcome a recommendation that an entire project be taken back to the drawing board and fundamentally re-designed, and it is unrealistic to expect [privacy impact assessment] practitioners to make such recommendations even where it is obvious to them that a different direction at an earlier stage would have been preferable.[362]

By contrast, "privacy by design"—an approach now advocated by privacy scholars and regulators, and mentioned for the first time as a legal

---

358 *See id.*

359 *See id.*

360 Adam Warren & Andrew Charlesworth, *Privacy Impact Assessment in the UK*, *in* PRIVACY IMPACT ASSESSMENT, *supra* note 357, at 205, 216–17 (finding privacy impact statements ("PIAs") are perceived as more effective when they prospectively identify risks prior to the establishment of systems and programs, are able to alter proposals, and are integrated into "workflows or quality assurance processes"); Kenneth A. Bamberger & Deirdre K. Mulligan, *PIA Requirements and Privacy Decision-Making in U.S. Government Agencies*, *in* PRIVACY IMPACT ASSESSMENTS, *supra* note 357, at 245-47 (discussing how PIA like environmental impact assessments appear to be more effective when they are required prior to program decisions and are aided by embedded substantive experts).

361 Waters, *supra* note 357, at 150–51.

362 *Id.* at 151.

goal in the draft European Privacy Regulation under debate[363]—requires a more decentralized and embedded approach to privacy.[364] Thus, "[t]rue 'privacy by design' will only be achieved when the instigators and designers of new systems recognise privacy at the outset as one of the variables that they need to consider," and privacy experts knowledgeable about technological and business choices must therefore be involved "when policies are being formulated and key choices are being made about how to meet organisational objectives."[365]

The managerialization of privacy evidenced in the responses of the leading U.S. and German corporations specifically reflect these approaches. The firms interviewed in those countries explained that incorporating privacy measures into other risk management systems both harnesses significant resources in the service of privacy and puts 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'/DPOs' participation in high-level strategy-setting fora, and their access to the highest levels of firm decisionmaking, provides a voice for privacy in setting firm priorities. And blending privacy into business-unit decisionmaking from the start also offers a means for transforming privacy from a cost or limit to a function that must be integrated, along with other core specifications, into each product or service.

The interviewed privacy leads stressed the importance of embedding expertise within business units and establishing specific staff who are personally responsible for privacy—typically through indirect reporting mechanisms. They viewed this as essential to institutionalizing privacy considerations in large decentralized organizations.[366] Literature on the

---

363 Ira S. Rubenstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1410 (2011).

364 *See* Waters, *supra* note 357, at 150–51.

365 *Id.*; *see also* John Edwards, *Privacy Impact Assessment in New Zealand—A Practitioner's Perspective*, *in* PRIVACY IMPACT ASSESSMENT, *supra* note 357, at 194–95 ("Once an information system to support the proposal is being designed, or business processes developed, a great many decisions, with varying degrees of impact on privacy, will need to be made.").

366 *See* David H. Flaherty, Privacy Impact Assessments: An Essential Tool for Data Protection, Presentation at the 22nd Annual Meeting of Privacy and Data Protection Officials, Venice, Sept. 27–30, 2000, *available at* http://aspe.hhs.gov/datacncl/flaherty.htm ("I conclude that the ideal privacy impact assessment of any project is prepared by someone from inside the project and with an up-front demonstration of just how it works or is supposed to work."); Blair Stewart, *Privacy Impact Assessment Towards a Better Informed*

relationship between formal structures and successful decentralized decisionmaking, moreover, further supports this claim,[367] as do studies of cognition. Those studies emphasize "interaction with others whose thought processes are not governed by the same culture or knowledge structures as the decision maker" as a principal means of forcing integration of secondary concerns that are in tension with an organisation's existing focus.[368]

The policies, training, and decisional tools provided to employees within the German and U.S. 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 periodically pull them out of their standard decisionmaking processes and focus 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.[369]

The role of the CPO/DPO as both a high-level insider and an actor

Process for Evaluating Privacy Issues Arising from New Technologies, 5 PRIVACY L. & POL'Y REP. 147, 147 (1999) ("PIA needs to be integrated into decision-making processes. For a government proposal, PIA might be integrated into departmental decision-making and appropriate cabinet processes . . . . The important thing is that PIA not be divorced from decision-making processes.").

367 W. RICHARD SCOTT, ORGANIZATIONS: RATIONAL, NATURAL AND OPEN SYSTEMS 262–63 (4th ed. 1998) (discussing scholarship suggesting that centralization and formalization may be viewed as alternative control mechanisms, as more formalized arrangements permit more decentralized decisionmaking).

368 *See* Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountibility in the Administrative State*, 56 DUKE L.J. 377, 443 (2006) (citing Chip Heath et al., *Cognitive Repairs: How Organizational Practices Can Compensate for Individual Shortcomings*, 20 RES. ORG. BEHAV. 1, 13 (1998) ("Often, organizations ensure that individuals weigh information effectively by forcing them to interact with others who might weigh the information differently.")); James P. Walsh, *Managerial and Organizational Cognition: Notes from a Trip Down Memory Lane*, 6 ORG. SCI. 280, 291 (1995) ("[R]esearch on the process of knowledge structure development suggests that a dramatically altered information environment is often the locus of knowledge structure change.").

369 Chris Argyris, *Good Communication that Blocks Learning*, HARV. BUS. REV. July-Aug. 1994, at 78.

who directly engages the privacy claims and justificatory frameworks of external stakeholders offers a model that our research indicates offers a means to promote more effective decision-making within the firm. This privacy officer model brings the perspectives of other organizations negotiating privacy into the firm. Bringing in outside perspectives is of great significance because of the connection between the legitimacy of firm behavior and the proper intuiting of evolving privacy norms, which—unlike prescriptive rules—are dynamic, are at times contradictory, can diverge both up and down from the law on the books, and vary contextually.[370] A CPO/DPO can therefore play an important "boundary-spanning" role,[371] serving both as a voice for privacy and as a powerful force within the firm, using a "privacy mindset" to spur careful internal decisionmaking in the face of pressure to focus on efficiency and profit.

2. *Privacy Managerialization and the Substance of Privacy Protection*

Moreover, by integrating discussions about the use of data from the very beginning of product or service development, this form of privacy "managerialization" offers a method for the consideration of privacy values beyond the simple vindication of individual notice and consent. It thus better permits the consideration of new threats to privacy unanticipated by traditional conceptions of fair information practices.

As privacy has become more salient in the political realm, and as technology has permeated all spheres of life, privacy's meaning itself has become increasingly contested.[372] The traditionally prevalent definition of privacy as "data protection," vindicated by compliance with mandates that individuals should control the disclosure and use of their personal information, has been increasingly criticized as insufficient to address concerns raised by technological shifts and globalization.[373]

The rhetoric of privacy as an individual right, with its concomitant procedural mechanisms to ensure the perfection of individual choice, has faced similar criticism.[374] So understood, the substantive interest in the protection of privacy is collapsed into a "right" to procedure.[375] Framing privacy protection as mechanisms that facilitate discrete decisions regarding access to or acquisition of data places the substantiation of

370 Dowling & Pfeffer, *supra* note 124, at 122.

371 Bamberger, *Regulation as Delegation*, *supra* note 368, at 444.

372 *See* NISSENBAUM, *supra* note 33, at 147–48.

373 *See id.* at 147–50.

374 COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 40 (2d ed. 2006).

375 *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY 226 (1995).

privacy's meaning in an individual's hands at one particular time, without knowledge or foresight about the changes in information treatment that future technologies and practices will bring.[376] Additionally, this framing often provides no substantive touchstone to guide the choices of those with far greater power to shape privacy's treatment—corporate actors shaping the systemic decisions about design choices that impact information usage.[377]

The prevalent forms of operationalizing privacy in leading U.S. and German firms reflect a recognition of the incompleteness and shortcomings of a reliance on formal notice and consent mechanisms alone to protect against real harms as rapid technology changes reduce the individual's power to isolate and identify the use of data that concerns them.[378] They highlight technological and market changes that indicate the frailty of an individual self-determination framework for guiding corporate decisions on how to address privacy issues raised by new products and services. Additionally, they permit the consideration of privacy concerns raised in path-breaking work by scholars from diverse fields, which increasingly promotes the consideration of substantive norms, social values, and evolving community practice—in addition to existing approaches emphasizing procedural tools to instantiate individual autonomy and personal choice—when evaluating privacy harms.[379] That scholarship suggests that privacy—and the impact of corporate behavior on it—must be understood by considering what users of information services bring to a transaction—the "mental model" they have of information "flows"—and whether a practice is unexpected in light of those understandings and therefore violative of public policy.[380] Such a focus on data flows—the ways in which information is actually used—in turn offers promise in creating a more robust conception of privacy values deserving of

376 *See* NISSENBAUM, *supra* note 33, at 148–50.

377 *See id.*

378 Scholars have thus noted the need for approaches to privacy that "transcend that of individual benefit" yet do not deny the centrality of the individual in privacy's formulation. BENNETT & RAAB, *supra* note 374, at 41–45. Another scholar has identified three reasons why "privacy as an individual right . . . provides a weak basis for formulating policy to protect privacy," namely, "it emphasizes the negative value of privacy; it establishes a conflict between the individual and society; and it fails to take into account the importance of large social and economic organizations." REGAN, *supra* note 375, at 212, 215 (1995). Regan also argues for a definition of privacy based on its benefit to "common, public, and collective purposes." *Id.* at 221.

379 *See supra* notes 376–378.

380 *See, e.g.*, NISSENBAUM, *supra* note 33, at 148–50.

defense.[381]

The emerging "managerialization" of privacy permits a diversification of the understandings of privacy[382] and the consideration of privacy values that may not be well protected by the notice and consent formalities. It does this by providing a means for considering the use of information throughout corporate decisionmaking regarding new technologies or business processes. This, in turn, renders more visible to corporate actors who make important systemic decisions about the technologies that affect privacy, the fact that the values embedded in technical systems and practices shape the range of privacy-protective choices individuals can and do make regarding interactions with those systems and practices,[383] and better avoids "set[s] of acts that will *together* harm other people."[384] This therefore reflects privacy's importance as a social good.

B. Accounting for Corporate Practices: Regulatory Field Elements and the Endogenaity or Exogenaity of Privacy Expertise

Formal regulation and institutional choices are insufficient to account for the differences and similarities in privacy's internal integration within firms in the four studied jurisdictions. The administrative structures of privacy governance, and definitions of privacy at work on the ground, in the United States and Germany diverge significantly.[385] By contrast, all three European countries share a common normative, lodestar, and data-protection approach.[386]

Identifying the factors that produce these results requires a more nuanced analysis of the regulatory environment—attending specifically to modalities of regulation and aspects of regulatory transparency—as well as a broader view of the range of external factors and actors that coalesce to shape corporate behavior. In particular, this subpart suggests that certain

---

381 *See* BENNETT, *supra* note 37, at 16.

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

383 *See supra* notes 181–183 and accompanying text.

384 *See* NISSENBAUM, *supra* note 33, at 242 (quoting DEREK PARFIT, REASONS AND PERSONS 86 (1986)) (explaining that embedded norms create practices "roughly oriented around" societal values and goals); *see also* Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 959 (1989) (offering a normative account of privacy that does not focus just on the protection of individuals, but also on protection of the community, and finding that privacy torts in the common law uphold social norms, which in turn contribute to both community and individual identity).

385 *See supra* notes 53–63, 284 and accompanying text.

386 *See supra* note 49 and accompanying text.

choices about regulatory practice, as well as other elements outside the formal data-protection regulation sphere, can combine to promote a greater perception of the necessity for firms to develop expertise about privacy's meaning—leading to the type of managerialization discussed above. This lies in contrast to a perception of privacy's demands as something shaped by expertise external to the firm and constituting an exogenous requirement with which firms must simply comply.

1. Regulatory Approaches: Agency Structure and the Specificity and Generality of Regulatory Mandates

Though there are enormous differences between the institutions that drive privacy in the two countries in which we found the greatest reliance on internal experts (Germany and the United States), there are important similarities in their modes of operation that our respondents indicated as critical to the similarities we found in corporate forms. Most basic are choices about the form of legal mandates, in terms of their level of "bindingness" and their level of specificity. While German law is more comprehensive and more detailed[387] than the broad "unfair or deceptive practices" mandate that empowers the FTC to police privacy in the United States,[388] it nonetheless requires interpretation and adaptation to address issues on the ground. Like the approach to privacy adopted by the FTC,[389] agencies throughout Germany largely play a consultative and advisory role with respect to private sector practices,[390] and do not have the authority to issue binding regulations.[391]

In particular, Germany's privacy legislation avoided a "top-heavy licensing and registration system for databanks."[392] This contrasted markedly with the approach taken by French national regulation, which

387 *See supra* note 284 and accompanying text.

388 *See supra* notes 218–219 and accompanying text.

389 The FTC has instead used enforcement mechanisms and other regulatory tools. *See supra* notes 220–222 and accompanying text.

390 *See* FLAHERTY, *supra* note 10, at 28; Bignami, *Cooperative Legalism*, *supra* note 270, at 429 (explaining that German privacy authorities have limited powers and can issue only nonbinding recommendations).

391 *See* FLAHERTY, *supra* note 10, at 28, 52 (describing attitude and approach of the federal Data Protection Commissioner ("DPC") as emphasizing "mediation, conciliation, and education" and explaining that the responsibility of the State Ministries of the Interior (LMIs) is implementation of data protection in the private sector, while the DPC has no direct role but "may express opinions"); Bignami, *Cooperative Legalism*, *supra* note 270, at 424, 429–30 (discussing that in Germany regulators were styled as ombudsmen who wielded soft powers of persuasion and describing the German system as one in which "self-regulation was central," and "rulemaking power was retained by the government").

392 Bignami, *Cooperative Legalism*, *supra* note 270, at 426.

"was the most formal and hierarchical of the early privacy systems," and whose vision of data protection focused primarily on "licensing, registration, and rulemaking powers" to develop detailed and formal conditions for the use of government and private-sector databanks.[393] This divergence in emphasis is further entrenched by the regulatory strategies utilized by the French and Spanish data protection agencies. The French privacy professionals interviewed, for example, described their sense that that their national regulator had built the largest regulatory infrastructure of any of the jurisdictions, and described the ways in which the regulator thereby focused on providing even more detailed and refined guidance to firms regarding the specific registration requirements with which they must comply.[394] And the Spanish national regulator used very public sanctions and other enforcement techniques to emphasize the centrality of formal requirements in the compliance with data protection mandates.[395] In both cases, the task of interpreting and fixing the meaning of regulatory mandates—and the relevant expertise necessary for that process—was situated largely within the regulator.

In both France and Spain corporations seeking to comply with privacy mandates were faced with a detailed set of registration and data-use requirements around which they were required to order their privacy function, whereas German and U.S. privacy leads, by contrast, reported that they found it both necessary and profitable to develop expertise regarding the operationalization of privacy within their own firms, and to engage other nongovernmental industry sectors in dialogue about emerging threats, to cultivate the joint development of best practices, and to evangelize for them. German law, from the outset, envisioned the private sector playing a crucial role in meeting statutory objectives, reflected both in the requirement that firms above a certain threshold appoint an independent internal data protection officer,[396] and in the practice of negotiating industry codes with regulators to set sector-based standards for behavior.[397] Each of these elements promoted a sense of value in developing privacy expertise within corporations.

The distinction between German and U.S. corporate understandings of what privacy compliance requires, and those of their French and Spanish counterparts, is reflected clearly in one comment by a French DPO with experience in each of the other jurisdictions. That DPO commented on a

393 *Id.* at 424.

394 *See supra* Part IV.C.1.

395 *See supra* Part IV.B.1.

396 *See supra* note 284 and accompanying text.

397 *See supra* note 221 and accompanying text.

puzzling phenomenon identified through our interview research: the fact that German DPOs consistently expressed confidence that they can, and do, comply with privacy mandates, while Spanish and French DPOs often indicated that full compliance was sometimes impossible, no matter how hard their efforts. The answer, he suggested, was that the German DPOs on the one hand, and the French and Spanish DPOs on the other, have traditionally not been "speaking of the same thing" when they use the word compliance—"[i]t depends on whether you view compliance as a process or as the outcomes." Thus the Germans, he felt, had made a "big move towards . . . the U.S. approach which is really becoming a compliance program like an ethics and compliance program," while the other jurisdictions relied more on formalities as evidence of compliance.

To be sure, this divergence may, in part, derive from differences in national traditions regarding openness to self-regulatory forms.[398] But it also directly reflects the insights of recent scholarship documenting the ways in which choices of regulatory form shape the allocation of expertise, between regulators and those they regulate, and the effectiveness of adaptation to changing threat models. Traditional regulation eschewed uncertainty in favor of regulatory specificity, emphasizing the centralization of both subject-matter expertise and enforcement in a government body, resulting in the promulgation of clear and concrete legal mandates.[399] Yet scholarship has documented shortcomings of such top-down approaches to governance,[400] and the manner in which reliance on compliance with a set of detailed provisions may frustrate, rather than further, underlying regulatory ends.[401] In particular, scholars suggest that such forms of regulation are poor at reducing the types of risk produced by a combination of factors,[402] ignore expertise and knowledge that exists in bodies outside the regulator (such as third parties, or regulated parties themselves),[403] skew the behavior of regulated organizations by fostering a process of bureaucratization that results in a "displacement of goals," by

398 Bignami, *Cooperative Legalism*, *supra* note 270, at 414 (contrasting Britain and Germany's reliance on self-regulation with other parts of the EU).

399 *See, e.g.*, *id.* at 424–26.

400 *See, e.g.*, Cass R. Sunstein, *Administrative Substance*, 1991 DUKE L.J. 607, 627 (citing failures in using "rigid, highly bureaucratized 'command-and-control' regulation" to govern numerous companies in a "diverse nation").

401 *See*, Bamberger, *Regulation as Delegation*, *supra* note 368, at 457–58.

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

403 *See, e.g.*, Bamberger, *Regulation as Delegation*, *supra* note 368, at 458–67.

which compliance with partial but specific rules—originally promulgated as a means for achieving a regulatory goal—becomes the singular end,[404] and lack, through their static nature, the ability to adapt to changing circumstances and new understandings.[405]

Together, this scholarship suggests ways that elements have cohered in both the U.S. and German privacy fields to spur new forms of privacy's operationalization within corporations. Specifically, it points to the regulators' roles in those jurisdictions in deploying broad legal mandates by means of a suite of "new governance" approaches that incorporate learning, dialogue, coordination, and process, as well as credibility, to center the public voice in shaping both the law's framing and the "compliance-plus"[406] mindset reflected by the interviewed privacy leaders. Thus it suggests that changes in the field have arisen because, rather than in spite, of regulatory ambiguity.[407] The incompleteness of privacy mandates permitted flexibility in the face of uncertainty and discretion in implementation, permitting heterogeneous methods of compliance in individual firm contexts.[408] This in turn allowed for enlisting the judgment of firm decisionmakers, drawing on their superior knowledge both about the ways risks manifest themselves in individual firm behaviors and business lines and about available risk-management capacities and processes.[409]

2. The Construction of the Privacy "Field": Openness to Stakeholder Participation, the Development of a "Social License" for Privacy, and the Importance for Corporate Attention to Privacy

Relatedly, the different national approaches to regulation shape the

---

404 *See, e.g.*, ROBERT K. MERTON, SOCIAL THEORY AND SOCIAL STRUCTURE 199 (rev. & enlarged ed. 1957).

405 *See* Alfred A. Marcus, *Implementing Externally Induced Innovations: A Comparison of Rule-Bound and Autonomous Approaches*, 31 ACAD. OF MGMT. J. 235, 250–51 (1988); Bamberger, *Regulation as Delegation*, *supra* note 368, at 445 (discussing studies indicating that making monitoring criteria well-specified and known to decisionmakers leads firms to take shortcuts in compliance).

406 *See supra* notes 161–162 and accompanying text.

407 THE LEGAL LIVES OF PRIVATE ORGANIZATIONS 1, 8 (Lauren B. Edelman & Mark C. Suchman, eds., 2007) ("[A]mbiguous mandates and uneven enforcement may actually *heighten* law's cognitive salience, as organizations struggle to make sense of legal uncertainties and to develop shared definitions of acceptable compliance").

408 *See id.*

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

extent to which a variety of stakeholders other than the regulator participate in the negotiation of privacy's meaning. The existence in both Germany and the United States of activist (and multiple) privacy regulators who demand forward-looking, dynamic interpretation of privacy mandates and emphasize collaborative methods to progress privacy practices, empower firm experts as well as other powerful social actors in the negotiation of privacy's meaning, and build pressure to comply with that meaning.[410]

Robert Kagan and other political scientists have demonstrated the potential power of nongovernmental stakeholders within a regulatory field in both increasing pressure on regulated parties to pursue public values, and in creating the meaning of those values (e.g., do they require simply compliance with formal law? Or something else? And what is that something else?).[411] This sort of participation can act as a "social license" that constrains corporate activity, reflecting "theories that emphasize the importance of a firm's social standing and in particular its economic stake in maintaining its reputation for . . . good citizenship."[412] The importance of such social forces, moreover, is underscored by the insights of public choice theory, which reveal the difficulties in creating a political constituency when the number of affected parties is large, and individual economic interest is small or uncertain,[413] as is the case with privacy. In particular, then, this participation can aggregate otherwise dispersed market, consumer, and advocacy pressures to reproduce the types of forces that scholars of corporate regulation flag as important in producing "beyond compliance" behavior: visibility, community concern, and threat to economic investment.[414] In these contexts behavior can be "shaped by a far broader range of stakeholders within the 'organizational field' than regulators alone."[415]

To be sure, the forms and breadth of independent third-party involvement in the U.S. and German privacy fields as reported by our interviewees differ notably. But both because of the need for refinement of legal mandates, and because of particular—albeit different—regulatory choices, the governance processes in Germany and the United States are

---

410 *See supra* notes 205–213, 220, 281, 283–286 and accompanying text.

411 NEIL GUNNINGHAM ET AL., SHADES OF GREEN: BUSINESS, REGULATION, AND ENVIRONMENT 136 (2003).

412 *Id.* at 147.

413 *Cf.* Harry G. Hutchison, *Choice, Progressive Values, and Corporate Law: A Reply to Greenfield*, 35 DEL. J. CORP. L. 437, 462 (2010) (explaining that the divergent interests of shareholders in the corporate context allow managers to take advantage of them and implement their own self-interested policies).

414 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 310.

415 GUNNINGHAM ET AL., *supra* note 411, at 147.

both relatively open to organized interests.[416] Thus in both countries, powerful constituencies vie with corporations over the meaning of firms' privacy obligations.

In the United States, the wide range of participatory procedures the FTC provided both publicized debates over privacy policy and enabled the rise of a movement of privacy advocates central to developing "frames that justify, dignify, and animate collective action"[417] around "privacy"—a "concept [that] leaves a lot to be desired" as "a clear organizational principle to frame political struggle."[418] Indeed, as one advocate explained, "[i]n the United States it's the agency debates that are really important."[419]

The U.S. CPOs we interviewed largely attributed their prominence and power within the firm to the perception of the importance of their role in negotiating, interpreting, and integrating this broader "license to operate," and to the way in which this new orientation places ethics and social obligations—as defined by noncorporate actors—within the scope of firm consideration.[420] Specifically, they were empowered by the ability to ask a broad range of questions about firm activities rather than simply defend such activities as legally permissible.[421] This facet of the CPO's job, they explained, "is of great significance because of the connection between the legitimacy of firm behavior and" a proper understanding 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."[422] As such, a CPO derives both independence and power from their important boundary-spanning role, serving both as a voice for privacy and as a trusted insider using a "privacy mindset" to spur mindful internal decisionmaking in the face of pressure to focus on efficiency and profit.

In Germany, interactions with regulators are predominantly one-on-one, though there were some sectoral and educational events organized

416 Bignami, *Cooperative Legalism*, *supra* note 270, at 414 (discussing the relative openness of Germany to "organized interests, involving informal consultation of interest group representatives" in comparison to France's reliance on "bureaucratic elites"); *see supra* note 220 and accompanying text.

417 BENNETT, THE PRIVACY ADVOCATES, *supra* note 111, at 1–2 (quoting SIDNEY G. TARROW, POWER IN MOVEMENT: SOCIAL MOVEMENTS AND CONTENTIOUS POLITICS 21 (2d ed. 1998)).

418 *Id.* at 2.

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

420 *See* Bamberger & Mulligan, *New Governance*, *supra* note 12, at 489–91, 501.

421 *See id.* at 489–93.

422 *Id.* at 501 (citing Dowling & Pfeffer, *supra* note 124, at 124).

through trade and professional associations.[423] But our German interviewees universally spoke of two independent institutional forces as central to determining privacy's meaning and the scope of permissible privacy behavior: the independent works councils that are required in each corporation under German corporations law,[424] and the independent Data Protection Officer mandated under national privacy law.[425] Fed by the informational events of breaches and fines, works councils, according to our interviewees, have become an important independent constituency, and a powerful legitimizing force for outside perspectives on the privacy practices of firms.[426]

Similarly, the DPO, whose job security, independence, and direct access to decisionmakers on the corporate board of trustees are protected robustly by law,[427] serves as an important force in bringing privacy concerns, and suggestions about privacy protection in the face of changing threats, to the highest levels of firm decisionmaking. The description of DPOs' roles, their power within the corporation, and their negotiation with other firm constituencies as both insider and outsider was strikingly similar to the descriptions of their U.S. counterparts—although their independence is, in the first instance, derived from legal mandates[428] rather than from social and market forces.

Together, however, our accounts suggest that the German works councils and the DPO offer an independent voice in privacy's negotiation parallel to that of independent civil society advocates in the United States, through both their legal right to shape practices related to workplace privacy, and their general advocacy and information-sharing around the public's privacy concerns.

Thus the dynamic multi-stakeholder processes in the United States, occurring against a backdrop of adversarial legalism and in an environment of powerful external stakeholders; and the co-regulatory cooperative legalism that dominates Germany, combined with strong regulations, a highly compliance oriented culture, and works councils, appear to drive similar firm behaviors. This suggests that we might we be far more suspicious of the ability to drive substantive aims at odds with the firms' bottom lines in the absence of either a strong and empowered civil society or a culture of, and a plausible risk of, litigation.

423 *See supra* Part IV.A.2.b.
424 *See supra* Part IV.A.1.
425 *See supra* note 276 and accompanying text.
426 *See supra* Part IV.A.1, 2.b.
427 *See supra* note 276 and accompanying text.
428 *See supra* note 276 and accompanying text.

Such independent forces in privacy's definition, by contrast, played little part in the accounts of our Spanish and French interviewees. In Spain, privacy leads did speak of the importance of consumer group empowerment through the creation of statutory causes of action with monetary penalties for privacy breaches and of this development's contribution to raising the level of attention firms paid to privacy by fomenting some greater connection between overall brand and privacy failures.[429] But this consumer-protection tool, they noted, was geared only towards strengthening pressure to comply with privacy formalities such as the documentation of consumer consent regarding the use of personal information.[430] It was unrelated to any sense that privacy might mandate the development of internal corporate expertise, or proactive risk-management in developing privacy practices.

French interviewees reported the absence of consistent third-party pressure altogether. While French privacy officers spoke of the nexus between privacy and the firm's obligations to society, there appears to be little actual opportunity for civil society actors to participate in conversations about how firms meet these obligations.[431] To be sure, French regulation has recently incorporated a number of efforts to enhance the role of the designated DPO/CIL in French corporations, and many corporations have begun to make such designations.[432] However, those efforts have not, on their own, resulted in the transformation of a privacy lead function in such a way as to change the attitude toward the development of robust expertise within the firm.

Finally, our interviews across diverse jurisdictions strongly suggest that privacy fares best, when it is entwined or nested in a broader substantive framework. This is true both in terms of fostering external social pressures for forward-looking privacy decisionmaking and with regard to making the case for allocating internal resources to the types of expertise and risk-management structures that facilitate such approaches. For example, privacy in the United States has benefited from its relationship to overall issues of marketplace fairness and consumer trust advanced by consumer protection agencies.[433] It has been integrated with other risk-management functions within corporations, enabling the leveraging of enhanced decisionmaking and auditing resources, and greater

---

[429] *See supra* Part IV.B.1.

[430] *See supra* Part IV.B.1.

[431] *See supra* Part IV.C.1.

[432] *See supra* Part IV.C.3.b.

[433] *See supra* notes 145, 154–158.

prominence within the firm.[434] In Germany, privacy in firms is nested within an overall focus on ethical behavior towards individuals, employees, and citizens—an approach that is advanced by works council representatives and dedicated privacy officers who operate in a framework that affords them independence.[435] Even in France, where corporate privacy structures are far more diverse,[436] the firms that have been most successful at devoting resources to internal decisionmaking structures have done so by increasing the constituency for privacy, and the resources available for its operationalization. They have done this by integrating privacy into existing ethics programs, or structures geared towards robust compliance with other, nonprivacy regulatory mandates or information security systems.[437] In these contexts, framing privacy as part of larger ethical or risk-management networks increased the number of stakeholders participating in the privacy discussion.

The exploration of stakeholders' relative empowerment through regulatory choice is especially significant in light of the increasingly central role of networks as key elements in social change—both in terms of privacy's form (will such networks exist?) and its substance (in terms of a renewed focus on privacy as an important element of open and free society, and the importance of corporate choices in supporting or hindering it). Given the entwinement of corporate and government privacy questions as the private sector provides the backbone networks for data mining, citizen control, policing, and intelligence gathering, these regulatory choices will significantly affect the locus of privacy expertise and decisionmaking. They will thus shape the resolution of other critical questions—i.e., will decisions be made only by the government or the firm? Or will third parties play an active role in shaping privacy norms as well?

3. Transparency and Corporate Attention to Privacy

Finally, and relatedly, a comparison of the four studied jurisdictions further underscores that the relative transparency of privacy is an important regulatory force creating pressure on firms to develop the internal expertise and structures necessary to develop forward-looking privacy practices, and to make decisions within the firm to increase the level of attention and resources devoted to privacy protection.

In particular, such a comparison suggests the elements of meaningful

---

434 *See supra* notes 159–160.

435 *See supra* note 245, Part IV.A.1.

436 *See supra* Part IV.C.1.

437 *See supra* Part IV.C.3.

transparency, in terms of promoting robust internal privacy practices. Scholars and policymakers have long promoted "informational regulation," or "regulation through disclosure," as means to "fortify either market mechanisms or political checks on private behavior" by mobilizing dispersed groups affected by relevant risks, and raising the level of attention to such risks within corporate decisionmaking.[438]

In a formal sense, much of European privacy regulation has been focused on a kind of transparency for decades: database registrations are an entrenched part of the European privacy landscape.[439] Yet while such requirements involve an aspiration to create a public record supporting knowledge and dialogue about privacy, there is little suggestion that they have succeeded. These routine filings are poorly designed to garner public attention or fuel public discourse, and reflect what one European scholar characterized as the "bureaucratization of data protection."[440]

While Germany's regulatory form predates the U.S. form by more than twenty years,[441] our interviewees from both countries described relatively similar levels of programmatic maturity, which is particularly striking given the longevity of the privacy officer requirement in German law. Indeed, as late as 1999, even Germany suffered from a process of bureaucratized transparency, and its data protection agencies shifted "uneasily between the image of data protection bureaucratization and an ombudsman role."[442]

It seems then, that events of recent years have shifted the German regulatory field, providing long existing regulatory requirements with new meaning and producing the level of attention within the firms identified to us as leaders, and the thick institutionalization we described. In the United States, this same sort of attention and thick institutionalization has arisen in a shorter window of time and without the same level of formal regulatory

438 Cass R. Sunstein, *Informational Regulation and Informational Standing:* Akins *and Beyond*, 147 U. PA. L. REV. 613, 613–14 (1999) (describing the shift in informational regulation as "one of the most striking developments in the last generation of American law").

439 *See supra* Part IV.C.1.

440 *See* Herbert Burkert, *Privacy-Data Protection: A German/European Perspective*, *in* PROC. 2ND SYMPOSIUM OF THE MAX PLANCK PROJECT GROUP ON THE LAW OF COMMON GOODS 62 (1999) (discussing the way agencies sometimes "convey the feeling that [they] regard themselves as being judged by the amount of pages they produce in these reports.").

441 *See* Bignami, *Cooperative Legalism*, *supra* note 270, at 422 ("Legislation was enacted in 1977 in Germany."); Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 273–76 (explaining the development of the FTC as an activist regulator in the 1990s and the emergence of breach notification laws in the 2000s).

442 Burkert, *supra* note 440 at 63 (internal citation omitted).

pressure.[443]

Our respondents repeatedly attributed these shifting privacy approaches to the development of a meaningful, and attention-focusing, form of informational transparency regarding privacy threats, and privacy risks. This form of transparency is distinct from its bureaucratic relation—it encompasses the type of "external shocks" that organizational theorists explain are particularly useful in focusing attention within firms, and enabling institutional capacity to respond to changing situations, and changing risks.[444]

In the United States, CPOs emphasized the importance of the FTC's public statements and roving enforcement activities both in offering evolving content to its privacy standards in new contexts, and in creating the pressure for forward-looking, dynamic, orientations in firms seeking to steer clear of legal troubles.[445] The FTC's public-facing activities tapped into the power of information, transparency, and publicity as regulatory forces, and offered a forum in which a host of public and private stakeholders could enter the public dialogue.[446] The Commission's emphasis on making privacy management practices and failures transparent surfaced metrics for assessing corporate activity over time[447] and benchmarks for improvement[448]—the type of measures that both permit external accountability and spur changes in organizational management.

Even in France, a number of our respondents described the importance of several recent CNIL inspections and enforcement actions, and the publicity that resulted, as critical in their decisions to begin exploring more robust internal considerations of privacy, to begin the process of designating a CIL, and to begin discussions about how to enhance the

443 *See supra* notes 149–150, 160.

444 Bamberger, *Regulation as Delegation*, *supra* note 368, at 439–40 (discussing the value of such external shocks in promoting organizational accountability).

445 Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 273–75.

446 *See supra* notes 219–222 and accompanying text.

447 *See* Michael C. Dorf & Charles F. Sabel, *A Constitution of Democratic Experimentalism*, 98 COLUM. L. REV. 267, 314–23, 403 (1998) (discussing how agencies can take advantage of their vantage point on the behavior of multiple firms to develop "rolling best practices" by collecting data from regulated entities about what works and what does not, and then disseminating that information back through education and capacity building); *see also* Karkkainen et al., *supra* note 354 (providing, in the environmental context, a model in which administrative agencies develop the architecture for gathering and analyzing information across local contexts as a part of the regulatory and education process).

448 *See* Sturm, *supra* note **Error! Bookmark not defined.**, at 492–519 (discussing the importance of benchmarks in fostering meaningful organizational change and improvement).

privacy function within the firm.[449]

Across several jurisdictions, moreover, the adoption of security breach notification requirements—started in the United States but becoming a common feature in Europe—has served as an important tool in creating informational events that place privacy in the public eye. According to our respondents, these informational events are most salient in the United States and Germany, although significant in Spain as well. In these three jurisdictions, news of breaches is received by distinct powerful constituencies: in Spain, sectoral consumer organizations;[450] in Germany, labor;[451] and in the United States, privacy and consumer advocates.[452]

Although in each country, then, the information generated by the breach laws empowered a powerful constituency, those different groups use the information in decidedly different ways. In Spain, unions and sector-oriented consumer organizations use DPA inquiries and fines, as well as breaches, opportunistically, as a way to raise broader grievances—particularly against high-visibility Spanish firms.[453] Companies viewed these actions as manipulative and illegitimate, and do not perceive them as being about the substance of privacy protection per se.[454] In addition, they were viewed by some as inevitable.[455] Consumer associations did not engage regulators or companies to reform corporate practices, but rather to extract fines.[456] The perception of corporations and actions of the consumer associations seem unlikely to promote a deep institutional commitment to privacy. In contrast, U.S. and German constituencies who make use of breach reports are largely concerned with the reform of privacy practices—or so it seems. In Germany, reported breaches—and the backstories—travel quickly through the works councils due to their potential connection to employees' interests. These internal players, with representatives on corporate boards, are an additional force that drives privacy within firms. In the United States, the country with the longest and richest experience with breach reporting, breach reporting laws have focused boards, shareholders, insurers, business partners, and consumers on privacy, increasing corporate attention and resources to privacy, and tying

449 *See supra* Part IV.C.3.

450 *See supra* Part IV.B.1.

451 *See supra* Part IV.A.1.

452 *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 276–77.

453 *See supra* Part IV.B.1.

454 *See supra* Part IV.B.1.

455 *See supra* Part IV.B.1.

456 *See supra* Part IV.B.1.

privacy protection to brand protection.[457]

4. *Initial Thoughts for Policy Choices*

The countries studied offer a range of regulatory institutions with vastly different powers and styles of influencing corporate behavior. In the United States, we identified the important role that soft-law techniques, wielded by the FTC, play in fleshing out the meaning of its ambiguous privacy mandate and, in the process, shaping a collective understanding of privacy among advocates, industry, academics and regulators.[458] While the FTC's function as a roving enforcement agency has been tremendously significant, its threat of coercive authority leverages an even more extensive role in developing a cross-field understanding of privacy through workshops, fact-finding investigations, and best practice oriented efforts.[459] While other countries studied lacked institutional tools and traditions to support multi-stakeholder engagements in the privacy area, openness and propensity for engagement with corporations and trade associations varied. In some instances, the interviewees explained, regulators interacted with corporations nearly exclusively through formal engagements such as filings, audits, complaint resolution, and enforcement. In others, DPOs reported that corporations engaged with regulators one-to-one or, less often, in the context of an industry-specific dialogue.

The extent to which regulatory structures allow or require firms to participate in defining privacy's governance influences the extent to which firms invest in privacy expertise. This breadth of investment is further shaped by privacy governance's openness to other stakeholders. The risk of privacy failures to brand, as well as bottom line, also influences the authority, independence, and resources privacy professionals can leverage. Regulatory forms and practices that make privacy endogenous to corporate strategy and risk management, yet constantly open to contest by other stakeholders (like those found in the United States and Germany), appear most likely to promote firm investment. In regulatory climates with limited interaction between regulators and corporations—particularly where informal interaction is limited—firms are more likely to perceive privacy as an exogenous force to which the firm must respond (as in the cases of Spain and France). In these climates, the regulator provides privacy's content, with little room for firm response or influence. In such environments, privacy is dealt with as a compliance activity—although not

457 *See supra* notes 205, 206–208.

458 *See supra* notes 220–222 and accompanying text.

459 *See supra* notes 220–222 and accompanying text.

always one that privacy managers expect can be discharged satisfactorily depending in large part on the positioning of the regulators. In firms with more regular engagement with regulators, corporations are more likely to view privacy as at least partially endogenous. Specifically, internal aspects of firm behavior inform privacy's definition and requirements, both prior to regulatory direction (as a result of the impact corporations can have on regulators' understandings of the business and technical environment in which privacy must operate), and after rules are proffered (as a result of the more-flexible regulatory directives such interactions yield). Regulatory practices we identify as associated with endogeneity engage the private sector and drive higher-level attention and greater development of internal expertise; by contrast, those associated with exogeneity yield an orientation toward legal compliance and compliance-oriented processes.

C. Suggestions About the Diffusion of Best Privacy Practices Across Jurisdiction

Finally, in thinking about Europe, our research indicates that more attention needs to be paid to the importance of nonregulatory, and non-European, influences on the ground that result in the diffusion—or lack thereof—of corporate structures and institutions that research suggests will be most adaptive in protecting privacy in the face of change.

Chief among the diffusion networks cited by our interviewees in every jurisdiction are networks of privacy professionals, including both the IAPP and local privacy professional groups that have developed in strong form over the last two or three years in France, Spain, and Germany. In every jurisdiction, our respondents credited these organizations, and the educational fora, conferences, certification and training programs, and other shared-learning events they coordinate, as critical sources for promulgating international corporate best practices.

In particular, numerous privacy leads in every jurisdiction described these professional groups as critical in disseminating and transmitting what they conceived of as successful "American" models for the role of "Chief Privacy Officers," and the internal corporate practices they spearhead. German DPOs described the way in which they used the resources and influence at their disposal as a result of the independence provided by national law to shape a DPO role modeled after their U.S. counterparts, while Spanish and French CPOs spoke about their attempts to try to parlay notions of best practices, increased publicity about privacy risks, and the leverage provided by industry privacy groups in order to command resources similar to those of CPOs in the United States.

Our interviewees' descriptions of the role that professional groups play in fast-tracking their privacy efforts to best-practices approaches (often modeled after the privacy apparatuses in U.S. firms) suggest that the account of European privacy regulation should be reformulated in an important way. The most sophisticated comparative analyses of European privacy law, like most comparative accounts of regulation, still look to regulators to explain the spread of regulatory tools and styles, at the expense of other players in the regulatory field. For example, Francesca Bignami's nuanced treatment of privacy policy concludes that "European regulatory styles are converging . . . . on a regulatory process that combines tough, legalistic administrative enforcement of government rules, extensive public pressure on industry actors to self-regulate, and low levels of litigation" which she calls "cooperative legalism."[460] In particular, Bignami credits regulators in Northern E.U. member states for the diffusion of self-regulatory approaches, including the adoption of corporate compliance officers and industry codes of conduct, and techniques such as privacy seals and privacy impact statements.[461] Abraham Newman, too, has centered his examination of policy diffusion on a strong network of Data Protection Authorities, suggesting their importance in the formulation of a unified privacy framework in the E.U. as well as changes in regulatory procedures and instruments in recent years.[462] Our research too suggests some convergence between regulator activity and overall changes in privacy approaches. Bignami's description of the spread of more flexible, new-governance-style tools and processes across Europe[463] resonates with our interviews, which indicated that such tools are solidly in place in Germany, and are in nascent stages elsewhere. Our interviews further suggest, however, that by their focus on regulators and regulatory networks,[464] these accounts misplace the source of diffusion and change in Europe.

In contrast, our interviews strongly suggest that the ultimate source of self-regulatory tools and procedures is neither European nor regulatory. Rather than attribute these developments to E.U. networks centered around DPAs, we find instead the spread of tools and techniques such as privacy

460 Bignami, *Cooperative Legalism*, *supra* note 270, at 412.

461 *Id.* at 435–40.

462 *See* NEWMAN, *supra* note 25, at 95 (documenting the formidable, and indeed outsized role, member state Data Protection Authorities played in the creation of the structure and requirements of the E.U. Directive).

463 Bignami, *Cooperative Legalism*, *supra* note 270, at 460.

464 *See id.* at 418 ("Within the European Union, the diffusion of policy ideas among national regulators is particularly intense because of the dense set of transnational policymaking networks that exist in virtually every area of social and economic governance.").

seals and privacy impact assessments—originating, and in fact far more advanced in deployment, in the United States[465]—have subsequently spread throughout corporate awareness through networks of privacy professionals spanning the public and private sectors.

Privacy seals, for example, began in the United States. While there is important work ongoing in various E.U. states and at the E.U. level, the first such efforts originated in the United States—while the European seal program dates from 2007,[466] the U.S. programs date from the late 1990s.[467] U.S. privacy professionals within U.S. corporations have largely advanced the use of seals in private sector privacy regulation,[468] with little regulator encouragement. Even the seals within Europe received important initial support from U.S. companies with an E.U. presence,[469] and, in fact, European data protection authorities were openly hostile to such seals in the context of the Safe Harbor negotiation with the United States around adequacy.[470]

---

465 *See* Bamberger & Mulligan, *Privacy on the Books, supra* note 6, at 263, 278; Press Release, European Commission, Electronic Identification, Signatures and Trust Services: Questions and Answers (June 4, 2012), *available at* http://europa.eu/rapid/press-release_MEMO-12-403_en.htm?locale=en (explaining that proposed regulations will help ameliorate the lack of seals used in the European Union); *infra* notes 467–471 and accompanying text.

466 *Privacy Seal—On Its Way From Kiel to Europe*, EUROPRISE (June 7, 2007), https://www.european-privacy-seal.eu/press-room/press-releases/privacy-seal-2013-on-its-way-from-kiel-to-europe.

467 *See* Colin J. Bennett and Deirdre K. Mulligan, The Governance of Privacy Through Codes of Conduct: International Lessons for U.S. Privacy Policy 21–22 (June 7-8, 2012) (unpublished manuscript) (on file with authors); *see also Website Privacy Services*, TRUSTE, http://www.truste.com/ (last visited June 11, 2013) (describing the TRUSTe seal); Press Release, Better Business Bureau, BBBOnLine Privacy Program Created to Enhance User Trust on the Internet (June 22, 1998), *available at* http://web.archive.org/web/20120128081208/http://www.bbb.org/us/article/bbbonline-privacy-program-created-to-enhance-user-trust-on-the-internet-163; *BBB Code of Business Practices (BBB Accreditation Standards)*, BBBONLINE, http://www.bbb.org/us/bbb-accreditation-standards (last visited June 11, 2013) (describing the launch of the Better Business Bureau's online privacy program in 1998).)

468 *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 6, at 263.

469 *See, e.g.*, Press Release, Educadium, Educadium Certified To Display TRUSTe EU Safe Harbor Seal (Mar. 11, 2010), *available at* http://www.educadium.com/press5.html ("The EU-US Safe Harbor Framework was developed by the U.S. Department of Commerce in concert with the European Commission to provide a framework for U.S. companies to comply with EU privacy directives protecting the personal information of European citizens.").

470 *See* Henry Farrell, *Privacy in the Digital Age: States, Private Actors and Hybrid Arrangements*, *in* GOVERNING GLOBAL ELECTRONIC NETWORKS: INTERNATIONAL PERSPECTIVES ON POLICY AND POWER 375, 388–89 (William J. Drake & Ernest J. Wilson III, eds., 2008). For a discussion of the emergence of seal programs during the Safe Harbor

Privacy Impact Assessments ("PIAs"), similarly, are of extra-European in origin. The general concept of impact assessments originated in the United States and United Kingdom, in the context of efforts to increase the efficiency of regulation by ensuring fidelity to regulatory aims at minimal cost.[471] The use of impact assessment in the realm of privacy regulation specifically originated in New Zealand and was first embraced by regulators in New Zealand, Australia, and Canada.[472]

By contrast, European use and discussion of PIAs has been historically limited. The most detailed history of this privacy tool concludes that "the term 'PIA' and the processes that a PIA involves have largely been developed in the Anglophone world" and found "virtually no material in the English language focused on PIAs in Member States of the European Union."[473] While the concept of 'Prior Checking' found in Article 20 of the 1995 E.U. Directive is consistent with the thrust of PIAs, such processes were spottily implemented in E.U. countries,[474] and in no case achieved the full expression found in laws and regulations of countries such as the United States, which adopted a PIA requirement for federal agencies in 2002.[475] Indeed, European regulators have been comparatively slow in requiring PIAs, and the first PIA handbook, developed in the U.K., was

negotiations between the E.U. Commission and the U.S. government, see Bennett & Mulligan, *supra* note 467.

471 David Parker, *(Regulatory) Impact Assessment and Better Regulation*, *in* PRIVACY IMPACT ASSESSMENT, *supra* note 357, at 77–81 (discussing rise of regulatory impact assessments in 1980s–90s in U.K. and U.S. under Thatcher and Reagan Administrations respectively and their push for smaller more effective government).

472 See David Wright & Paul De Hert, *Introduction to Privacy Impact Assessment*, *in* PRIVACY IMPACT ASSESSMENT, *supra* note 357, at 3, 8–9, tbl. 1.1 (stating "Privacy impact assessment may seem to be a new instrument in Europe" and discussing the history and spread of privacy impact assessments, specifically early use and development in non-E.U. jurisdictions including United States, Canada, Hong Kong, and New Zealand); *accord* Roger Clarke, *Privacy Impact Assessment: Its Origins and Development*, 25 COMPUTER L. & SECURITY REV. 123, 123-35; Flaherty, *supra* note 366; Stewart, *supra* note 366, at147 (noting that PIAs have been implemented in jurisdictions of New Zealand since the early 1990s).

473 Clarke, *supra* note 472, at 123–35.

474 *Id.*

475 *See* Pub. L. No. 107-347, § 208, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 (2006)) (requiring agencies to conduct a PIA before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form"); *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OMB (Sept. 26, 2003), http://www.whitehouse.gov/omb/memoranda/m03-22.html. For a discussion of the PIA and its use within federal agencies see Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75 (2008).

published in December 2007.[476] The European Commission's first call for PIAs was later still, coming in the context of radio frequency identification ("RFID") tags, where the Commission called upon the Member States to provide input to the Article 29 Data Protection Working Party for development of a privacy impact assessment framework to govern deployment.[477] Only recently has the European Commission begun to embrace self-regulatory strategies more fully. In recent years the call for PIAs, particularly in the context of the broader "privacy by design" framework, has intensified.[478] For example, the European Parliament, in its 2010 resolution on passenger name records, said that "any new legislative instrument must be preceded by a Privacy Impact Assessment and a proportionality test."[479] And in July of that same year, Vice-President Viviane Reding said that "Businesses and public authorities . . . . will need to better assume their responsibilities by putting in place certain mechanisms such as the appointment of Data Protection Officers, the carrying out of Privacy Impact Assessments and applying a 'Privacy by Design' approach."[480]

The diffusion of policy instruments, as well as models of privacy leadership and corporate best practices, from the United States to the E.U. suggests the importance of transnational networks of privacy professionals and the associations and meetings that convene them. Professionals within the private sector are key actors in the regulation of privacy, transferring privacy tools and approaches from one jurisdiction to another through conferences and trainings, interactions with regulators, and through contractual clauses and binding corporate rules.

In addition, the pattern of transition in privacy poses a question as to whether the U.S. adversary system is an important testing and development

476 [U.K.] Information Commissioners Office (ICO), *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, December 2007, Version 2.0, June 2009.

477 Commission Recommendation of 12 May 2009 on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio–Frequency Identification, 2009 O.J. (L 122) 47, 50.

478 *See* Waters, *supra* note 357, at 150–51.

479 European Parliament, Resolution of 5 May 2010 on the Launch of Negotiations for Passenger Name Record (PNR) Agreements with the United States, Australia and Canada, 2011 O.J. (C 81 E) 70, 73. The Framework was approved by the Article 29 Working Party in February 2011. Press Release, Article 29 Data Protection Working Party, European DPAs Adopt Opinion on RFID Privacy Impact Assessment Framework (Feb. 16, 2011), *available at* http://ec.europa.eu/justice/policies/privacy/news/docs/pr_16_02_11_en.pdf.

480 Press Release, Viviane Reding, Vice President and Comm'r, European Comm'n, Justice, Fundamental Rights and Citizenship, Towards a True Single Market of Data Protection 3 (July 14, 2010), *available at* http://europa.eu/rapid/press-release_SPEECH-10-386_en.htm.

ground that foments the creation of expertise in the private sector and, perhaps equally importantly, the privacy bar—and even other outside experts such as auditing and risk management professionals—that then is transferred to multinational corporations, trade and professional associations, and service providers who are adept at using these methods and tools and, at times, have a deep financial interest in promulgating their wide adoption. If this is so, it would suggest that new governance strategies may help to promote social values in a particularly important way because they align the interests—power and economic resources—of firm professionals with a more robust, rather than formulaic, expression of those values within the firm.

CONCLUSION

As the European Union debates the contours of a new privacy regulation designed to preempt variation in national regulation, it is crucial that European policymakers consider lessons regarding changing privacy threat models, corporate successes and failures in addressing those threats, and the ways in which successes have been spurred by regulatory choices, and spread within and across jurisdictions. There are some grounds for optimism: regulators increasingly speak about the need for "Privacy by Design"—the notion that privacy should be built in to technical and organizational decisionmaking regarding the design and operation of information and communication technologies—and the draft regulation specifically requires data controllers to "implement appropriate technical and organisational measures and procedures in such a way that . . . processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."[481] Yet this nod to the importance of organizational structures geared to considering privacy in business decisions is strikingly sparse when compared to the draft document's lengthy articulation of the substantive notions about individual rights in informational self-determination.[482] Additionally, it signals nothing too new; the language largely echoes the Data Protection Directive's existing provision requiring data controllers to implement technical and organizational measures in the design and operation of information technologies.[483]

481 *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, at 57, COM (2012) 11 final (Jan. 25, 2012).

482 *Id.* at .17–39.

483 *See* Council Directive 95/46, art. 17(1), 1995 O.J. (L 281) 31, 43 (EC) (requiring

This initial slice of empirical research on European privacy practices "on the ground" suggests that a greater regulatory purposiveness is needed in terms of ensuring that the next generation of privacy protection preserves and enhances the successes of the last. A true account of European privacy involves not just one story, but multiple stories generated by jurisdictional variance. Regulators must recognize that fact, and the lessons that can be learned from it, in their efforts to protect privacy. Moreover, success in promoting the development of robust corporate expertise regarding privacy protection, the allocation of firm resources to privacy decisionmaking, and vigorous engagement with rapidly-evolving privacy challenges, requires a focus on a complicated and contingent set of factors, involving regulatory approaches, the enlistment of networks of societal actors, and the development of independent voices invested in the negotiation of privacy's meaning. That account requires a far more granular, and bottom-up, analysis of both differences in national practice and the forces on the ground that result in the diffusion—or lack thereof—of corporate structures and institutions that research suggests are most adaptive in protecting privacy in the face of change.

data controllers to implement appropriate technical and organizational measures for safeguarding personal data).