Notre Dame Law Review Reflection

Volume 96 | Issue 4 Article 4

5-19-2021

Outsourcing Privacy

Ari Ezra Waldman
Professor of Law and Computer Science and Director, Center for Law, Innovation, and Creativity, Northeastern University School of Law and Khoury College of Computer Sciences. PhD, Columbia University; JD, Harvard Law School

OUTSOURCING PRIVACY

*Ari Ezra Waldman**

INTRODUCTION

Managerialism is an ideological framework that calls for institutions to be organized around the values of efficiency, productivity, and innovation.[1] It prioritizes the logics of efficient management over social welfare, inclusivity, and egalitarianism. Managerialized governmental institutions are evaluated as if they are for-profit businesses. Managerialized corporations are focused on leanness and efficiency rather than, say, social responsibility or providing employees with adequate salaries and benefits.[2]

In her book, *Between Truth and Power*, Julie Cohen deftly describes how managerial values and practices in judicial and regulatory institutions have helped entrench the power of corporations in the information economy.[3] For example, managerialized judicial processes, like expedited discovery rules and the pressure to settle rather than litigate claims, make it difficult for privacy plaintiffs to seek justice through the courts.[4] Courts, too, have been eager to outsource their adjudicative responsibilities to entities outside the

* Professor of Law and Computer Science and Director, Center for Law, Innovation, and Creativity, Northeastern University School of Law and Khoury College of Computer Sciences. PhD, Columbia University; JD, Harvard Law School. Special thanks to Julie Cohen, whose brilliant and insightful work consistently and ceaselessly inspires my own. Thanks also to Danielle Keats Citron, Woodrow Hartzog, Margot Kaminski, Orly Lobel, Bill McGeveran, Mark McKenna, Deirdre Mulligan, Frank Pasquale, and Neil Richards, as well as the editors of the *Notre Dame Law Review Reflection*. All errors—none of which have been outsourced—are my own.

1 JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 144–45 (2019).

2 *Id.* at 145.

3 *Id.* at 154–67. I am using the phrase "information industry" to refer to companies that profit off the data they collect from their customers or internet and technology users in general. It includes both Big Tech—Apple, Amazon, Facebook, Google, and Microsoft—as well as data brokers and companies—like those in retail and finance—who may have developed with a primary focus elsewhere but nonetheless reap profits from the collection, processing, and commodification of information about us.

4 *See id.* at 154.

judicial process in order to make litigating claims more efficient: they enforce boilerplate forced arbitration clauses that remove claims from courts entirely;[5] rely on settlements or consent decrees that deputize regulated entities to monitor and police themselves;[6] and outsource judicial decisionmaking to mediators and arbitrators who hear evidence, consider legal arguments, and issue binding orders.[7]

Just like managerialized judicial institutions are making it more difficult for individuals to vindicate their rights against modern corporations generally, managerialism in the privacy space is also undermining the ability of privacy law to rein in excessive corporate data extraction. Managerialized privacy compliance focuses on minimizing the law's impact on product innovation rather than on substantive adherence to the goals of privacy law. As such, the information industry has created compliance structures and mechanisms—policies, offices, impact assessments, audits, trainings, and so forth—that bear resemblance to legal structures, but are actually compliance in name only.[8] They are, to use Lauren Edelman's phrase, merely symbolic, standing in place of actual adherence to privacy law and leveraged as misleading evidence of compliance as data-extractive behavior continues unabated behind the scenes.[9] Managerialized regulatory institutions are far more likely to defer to these merely symbolic compliance mechanisms than those focused on vindicating the rights of consumers: they are easy heuristics, they make adjudication simple, they permit a light regulatory touch, and they do not stand in the way of private innovation. As Cohen argues persuasively, managerialized legal structures are complicit in the ballooning and unaccountable power of the information industry.[10]

An underappreciated part of the narrative of privacy managerialism—and the focus of this Essay—is the information industry's increasing tendency to outsource privacy compliance responsibilities to technology vendors. In the last three years alone, the International Association of Privacy Professionals (IAPP) has identified more than 250 companies in the privacy

5 *Id.* at 155–56.

6 *See id.* at 161–63.

7 *See, e.g.*, CHARLES GARDNER GEYH, COURTING PERIL: THE POLITICAL TRANSFORMATION OF THE AMERICAN JUDICIARY 16–43 (2016); Jean R. Sternlight, *The Rise and Spread of Mandatory Arbitration as a Substitute for the Jury Trial*, 38 U.S.F. L. REV. 17, 20 (2003) (binding arbitration takes away the opportunity for a trial); Jean R. Sternlight, *Rethinking the Constitutionality of the Supreme Court's Preference for Binding Arbitration: A Fresh Assessment of Jury Trial, Separation of Powers, and Due Process Concerns*, 72 TUL. L. REV. 1, 5 (1997).

8 Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 776–77 (2020) [hereinafter Waldman, *Privacy Law's*].

9 *See* LAUREN EDELMAN, WORKING LAW: COURTS, CORPORATIONS, AND SYMBOLIC CIVIL RIGHTS 32 (2016).

10 COHEN, *supra* note 1, at 154–64.

technology vendor market.[11] These companies market their products as tools to help companies comply with new privacy laws like the General Data Protection Regulation (GDPR),[12] with consent orders from the Federal Trade Commission (FTC),[13] and with other privacy rules from around the world. They do so by building compliance templates, pre-completed assessment forms, and monitoring consents, among many other things. As such, many of these companies are doing far more than helping companies identify the data they have or answer data access requests; many of them are instantiating their own definitions and interpretations of complex privacy laws into the technologies they create and doing so only with managerial values in mind. This undermines privacy law in four ways: it creates asymmetry between large technology companies and their smaller competitors, it makes privacy law underinclusive by limiting it to those requirements that can be written into code, it erodes expertise by outsourcing human work to artificial intelligence and automated systems, and it creates a "black box" that undermines accountability.

This Essay proceeds as follows. In Part I, I create a partial taxonomy of privacy technology vendors. The purpose of this section is to use primary source material from the vendors themselves to show that some of them are necessarily interpreting legal requirements and coding them into their products, even when they suggest they aren't. Part II teases out the implications of privacy managerialism and privacy compliance outsourcing, in particular, focusing on the four primary concerns of asymmetry, underinclusiveness, expertise, and accountability. The Essay concludes on a cautionary note: if it is ever legitimate, outsourcing is traditionally most often used for corporate functions and responsibilities that "lie outside the firm's core . . . competencies."[14] What does it say about companies in the information industry, many of which remind us that our "privacy is important" to them, and privacy professionals' trade organizations like the IAPP, that they are so eager to outsource their privacy compliance responsibilities? Outsourcing privacy is, therefore, not only an example of privacy managerialism, but also a symptom of privacy's systematic marginalization throughout the information industry.

11 IAPP, 2019 PRIVACY TECH VENDOR REPORT 3–4 (V.3.2 ed. 2019), https://iapp.org/media/pdf/resource_center/2019TechVendorReport.pdf [hereinafter TECH VENDOR REPORT].

12 *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) [hereinafter GDPR].

13 *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 606–09 (2014).

14 COHEN, *supra* note 1, at 157.

I. PRIVACY TECHNOLOGY VENDORS

Outsourcing usually involves shifting a specific, limited corporate activity that used to be done in-house to a third party because that third party can do it more efficiently and less expensively.[15] Routine functions—custodial, catering, and security, among many others—as well as highly specialized tasks—accounting, human resources, and informational technology, for example—are often outsourced when they are outside the "core competencies" of the firm.[16] This includes legal tasks as well, like when companies hire outside litigators and legal counselors. Increasingly, though, as technology outsourcing becomes more widespread in general, companies in the information industry are outsourcing legal and quasi-legal decisions to algorithmic systems, from content moderation to privacy compliance.[17]

The IAPP has identified ten categories of tasks performed by privacy technology vendors: assessment management, which involves automating privacy impact assessments and demonstrating compliance; consent management, which helps companies ask for and track user consents; incident response, which assists with responding to data breaches; privacy information management, which summarizes privacy law developments; de-identification and pseudonymization, which allow companies to process data; data mapping, which helps companies identify how their data is being used; website scanning, which reviews company websites to determine what kind of trackers they're using; activity monitoring, which tracks who has access to what data; data discovery, which tells companies what information they have; and enterprise communications, which facilitate internal communications to avoid leaks.[18] Of the 259 vendors profiled in its 2019 Privacy Tech Vendor Report, none do all of these tasks, three report that they can perform nine of them, and seventy-two do only one of them. The most common task performed by technology vendors is data mapping (114); the fewest vendors do website scanning (30).[19]

But this taxonomy elides what makes this vendor market troublesome. In outsourcing privacy compliance, the information industry is not just shifting responsibilities. It is changing the medium through which special kinds of responsibilities—interpretation and implementation of legal rules—are performed—namely, from humans to technology.

---

15 See Michael Quinlan, *Labour Market Restructuring in Industrialised Societies: An Overview*, 9 ECON. & LAB. RELS. REV. 1, 12 (1998).

16 See James Brian Quinn, *Strategic Outsourcing: Leveraging Knowledge Capabilities*, SLOAN MGMT. REV., Summer 1999, at 9, 12; Peter Gottschalk & Hans Solli-Saether, *Critical Success Factors from IT Outsourcing Theories: An Empirical Study*, 105 INDUS. MGMT. & DATA SYS. 685, 686 (2005).

17 *See, e.g.*, Evelyn Douek, *Governing Online Speech: From "Posts-As-Trumps" to Proportionality & Probability*, 121 COLUM. L. REV. (forthcoming 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3679607.

18 *See* TECH VENDOR REPORT, *supra* note 11, at 5.

19 *Id.* at 11–19.

JLINC Labs, for example, claims its consent management software "makes it easy to comply with any data-related legislation."[20] Nymity's privacy compliance technology claims that it is "GDPR Ready" and helps "organizations attain, maintain and demonstrate ongoing compliance."[21] FairWarning, which markets privacy and security solutions to health care providers, claims, without evidence, that its program fully complies with Article 25 of the GDPR and "fully addresses" five of the Phase 2 HIPAA Audit protocol elements and "partially addresses" twenty-six more.[22] ZLTech also offers "GDPR Ready Solutions," and explicitly claims that its tools to identify, minimize, and govern personal data uses will make clients compliant with multiple parts of the GDPR.[23] Market puffery or not, these claims suggest that compliance vendors are instantiating particular visions of what the law requires into their technologies.

---

20 Ari Waldman, *When We Outsource Privacy Compliance, We May Undermine Privacy Protection*, PROMARKET (Apr. 15, 2019), https://promarket.org/2019/04/15/when-we-outsource-privacy-compliance-we-may-undermine-privacy-protection/.

21 *See* NYMITY, PRIVACY COMPLIANCE SOFTWARE, https://web.archive.org/web/20180905234153/https://info.nymity.com/hubfs/Nymity%20Story/Nymity%20Story.pdf?pdf=Nymity-Story (last visited Apr. 24, 2021). *See generally How Technology Can Help Achieve GDPR Compliance?*, RISKPIN (June 25, 2018), http://blog.riskpin.com/2018/06/25/how-technology-can-help-achieve-gdpr-compliance/ ("GDPR Compliance tools like Nymity . . . help organisations keep abreast of upcoming compliance changes making them better prepared to meet compliance requirements."); NYMITY, FRAMEWORK FOR DEMONSTRABLE GDPR COMPLIANCE (2018), https://info.nymity.com/hubfs/Landing%20Pages/GDPR%20Toolkit/Accountability_Roadmap_for_Demonstrable_GDPR_Compliance.pdf (detailing specific GDPR Articles, including Articles 15 (right of access), 17 (right to erasure, or "right to be forgotten"), 18 (right to restriction of processing), 25 (right to privacy by design and by default), 30 (reporting), and 32 (security of processing)). *See also* NYMITY, REPORTING ON GDPR COMPLIANCE 9 (2018), https://info.nymity.com/hubfs/Landing%20Pages/Reporting%20on%20GDPR%20Compliance/Nymity%20Regulator%20Ready%20Reporting%20Whitepaper-%2020180713.pdf (implying use of toolkit will comply with Article 30 reporting requirements).

22 *See* IMPRIVATA, IMPRIVATA FAIRWARNING MAPPING TO GDPR 2, https://www.imprivata.com/resources/whitepapers/how-fairwarning-helps-you-meet-gdpr (last visited Apr. 24, 2021); IMPRIVATA, IMPRIVATA FAIRWARNING CAPABILITIES MAPPING TO HIPAA 1, https://www.imprivata.com/resources/whitepapers/how-fairwarning-fulfills-on-hipaa (last visited Apr. 24, 2021); *see also OCR Launches Phase 2 of HIPAA Audit Program*, DEP'T HEALTH & HUM. SERVS. (Mar. 21, 2016), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html?language=es (noting that Phase 2 audits ensure that entities covered by HIPAA comply with "Privacy, Security, and Breach Notification Rules").

23 *ZL Technologies Announces GDPR Ready Solutions*, ZLTECH (Oct. 30, 2017), https://www.zlti.com/press-releases/zl-technologies-announces-gdpr-ready-solutions.

A. Assessment Management

Assessment management software, provided by 103 companies on the IAPP's list, can automate the day-to-day work of privacy programs, including operationalizing privacy impact assessments (PIAs), training employees, and completing and submitting compliance documents to regulators.[24] PIAs, first deployed in the government context, are formal "analys[es] of how personally identifiable information is collected, used, [and] shared."[25] The 2002 E-Government Act requires all federal agencies to conduct and issue PIAs "for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information,"[26] and they are expressly required by the GDPR.[27] The FTC also requires regulated entities to engage in ongoing monitoring and reporting for up to twenty years after signing a consent decree.[28]

That means that PIAs have to meet some legal criteria to constitute compliance. But, as several scholars have noted, privacy law is rather vague on this point, rarely stating PIA and other requirements explicitly and precisely.[29] Therefore, outsourced PIAs necessarily reflect vendor interpretations of unclear legal rules. If they want to comply with the law, they have to understand provisions in the GDPR and in FTC consent decrees, as well as integrate guidance from the Data Protection Board and any recent outcomes of investigations and litigations. According to the IAPP, although most companies use their in-house legal team to conduct PIAs, fifteen percent use a vendor-designed template that may be different than ones created by

24 *See* TECH VENDOR REPORT, *supra* note 11, at 5–7.

25 *Privacy Impact Assessments*, FED. TRADE COMM'N, https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments (last visited Apr. 24, 2021) [hereinafter *Assessments*]. PIAs are not without their challenges. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *PIA Requirements and Privacy Decision-Making in US Government Agencies*, *in* PRIVACY IMPACT ASSESSMENT 225, 226, 230–35 (David Wright & Paul De Hert eds., 2012).

26 DEP'T HOMELAND SEC., PRIVACY IMPACT ASSESSMENTS 1 (2010), https://www.dhs.gov/publication/privacy-impact-assessment-guidance.

27 *See* GDPR, *supra* note 12, art. 35.

28 *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Says Hello to 1996 by Waving Goodbye to Thousands of Administrative Orders that Are at Least 20 Years Old (Dec. 20, 1995), http://www.ftc.gov/news-events/press-releases/1995/12/ftc-says-hello-1996-waving-goodbye-thousands-administrative (noting both existing and future consent orders would last twenty years); *see also, e.g.*, Sony BMG Music Ent., 062-3019 F.T.C., 10 (June 28, 2007), https://www.ftc.gov/sites/default/files/documents/cases/2007/06/0623019do070629.pdf (decision and order) (noting twenty-year time frame).

29 *See* Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1597–98 (2019) (noting that some of the provisions of the GDPR are "deliberately vague" and become less vague over time with interpretations from government agencies); Solove & Hartzog, *supra* note 13, at 625.

lawyers or made available by government agencies.[30] But vendor-designed templates necessarily make legal conclusions, often without lawyers.

Assessment management vendors promise that their tools will automate legal compliance beyond PIAs. Nymity, for example, offers a "software solution for templating" to create an automated "privacy program . . . made up of policies, procedures, and other accountability mechanisms."[31] Its templates are "60 percent complete, flexible to the needs" and business focus of the company, making regulatory "compliance easy."[32] CyberSaint marketed "audit-ready reports . . . that require no human effort to produce."[33] AuraQuantic's "GDPR Accelerator" calls itself an "All in 1" complete compliance management tool with templates, logs, and systems "with predesigned processes to comply with the regulation."[34] And Compliance Point promises that its OnePoint platform "enables organizations to implement a unified approach to complying with . . . HIPAA, . . . FISMA [(Federal Information Security Management Act)], . . . Cyber Security Framework, GDPR, and more."[35] Many other technology vendors make similar guarantees.[36]

It is easy to see how outsourcing assessment management requires outsourcing legal interpretations. If reports are "audit-ready," they have to

30 *See* IAPP & TRUSTARC, MEASURING PRIVACY OPERATIONS 12 (2018), https://iapp.org/media/pdf/resource_center/IAPP-Measuring-Privacy-Operations-FINAL.pdf [hereinafter MEASURING PRIVACY] (describing prevalence of Data Protection Impact Assessments (DPIAs), which are very similar to PIAs).

31 NYMITY, 2018 PRIVACY COMPLIANCE SOFTWARE BUYER'S GUIDE 9 (2018), https://info.nymity.com/hubfs/2018%20Privacy%20Compliance%20Software%20Buyers%20Guide/Nymity-Buyers-Guide-GDPR-Edition.pdf?t=1525179547972 (suggesting that its templating software will allow clients to create their privacy programs).

32 Interview with Paul Lewis, FIP, CIPM, CIPT, CIPP/C, CISSP, Senior Privacy Office Solutions Advisor, Nymity, in Washington, D.C. (Feb. 27, 2018) (notes on file with author).

33 Steven Bowcut, *Automation and Visibility to Your Compliance and Risk Management Program*, BRILLIANCE SEC. MAG. (Apr. 2, 2020), https://brilliancesecuritymagazine.com/compliance/automation-and-visibility-to-your-compliance-and-risk-management-program/.

34 *GDPR: Accelerate Compliance in Record Time*, AURAQUANITC, https://www.auraquantic.com/gdpr/ (last visited Apr. 24, 2021).

35 *OnePoint*, COMPLIANCEPOINT, https://www.compliancepoint.com/onepoint (last visited Apr. 24, 2021).

36 *See, e.g.*, *GDPR Compliance*, MENTIS, https://www.mentisinc.com/gdpr-compliance/ (last visited Apr. 24, 2021) (marketing its various platforms as compliant with several GDPR provisions); *Case Studies*, CROWNPEAK, https://www.crownpeak.com/resources/case-studies/ (last visited Apr. 24, 2021) (listing a diverse array of companies from Toyota to JAMS); *Tag Monitoring and Management*, CROWNPEAK, https://www.crownpeak.com/products/monitoring-solutions/tag-auditor-with-trackermap (last visited Apr. 24, 2021) (Evidon (now Crownpeak) offering website tracking to comply with GDPR, CalOPPA, and other statutes, among other tools); *The Consent Solution for Enterprise-Grade Digital Experiences*, CROWNPEAK, https://www.crownpeak.com/products/consent-solutions/universal-consent-platform (last visited Apr. 24, 2021) (noting consent solutions say they "ensur[e]" compliance).

include the kinds of questions regulators require of independent audits. Systems that "comply with regulations" have to understand what those regulations actually require. And any platform that regularly updates a company's compliance status requires a benchmark of what constitutes compliance in the first place. Therefore, although these technologies are not overtly offering legal advice like outside counsel, they are nevertheless embedded with particular assumptions and interpretations of legal rules.

B. Consent Managers

The eighty-two vendors that offer consent management software can track and record user affirmative consent.[37] To effectively assist with compliance, however, these tools have to be coded to recognize, distinguish, and obtain the different kinds of legal consents—explicit,[38] unambiguous,[39] verifiable,[40] written and informed,[41] and so forth—all of which have (different) legal definitions. After all, notice-and-consent remains at the foundation of privacy law in the United States. And although scholars have argued that the GDPR is not a consent-based statute,[42] consent is one of the lawful bases on which companies can collect and process customer data.[43] The Data Protection Board and national data protection agencies have also issued opinion documents detailing the factual indicia of valid consent.[44] The European Court of Justice has also issued rulings on the legitimacy of pre-checked boxes for cookie consents.[45]

Despite that complexity, vendors often sell themselves as comprehensive consent solutions. PossibleNow collects express consent, cookie consent, and other preferences and provides a paper trail to "ensur[e] compliance with"

37 *See* TECH VENDOR REPORT, *supra* note 11, at 5, 7.

38 *See, e.g.*, CAL. FIN. CODE § 4052.5 (West 2020) (requiring explicit consent before financial companies can share customer information); GDPR, *supra* note 12, art. 9(2)(a).

39 *See, e.g.*, GDPR, *supra* note 12, art. 4(11) (consent must be unambiguous).

40 *See, e.g.*, Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, § 1303(b)(1)(A)(ii), 112 Stat. 2681-728, 2681-730 (codified as amended at 15 U.S.C. § 6502(b)(1)(A)(ii)) (requiring "verifiable parental consent").

41 *See, e.g.*, ALASKA STAT. § 18.13.010(c) (2020) ("A general authorization for the release of medical records or medical information may not be construed as the informed and written consent required by this [law].").

42 *See* Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENVER L. REV. 93, 106–12 (2020).

43 *See* GDPR, *supra* note 12, art. 6(1)(a).

44 EUR. DATA PROT. BD., GUIDELINES 05/2020 ON CONSENT UNDER REGULATION 2016/679, ¶¶ 11–105 (Version 1.1 ed. 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

45 *See, e.g.*, Case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände–Verbraucherzentrale Bundesverband eV v. Planet 49 GmbH, ECLI:EU:C:2019:801, ¶ 65 (Oct. 1, 2019) (concluding that a pre-checked checkbox does not constitute valid consent for information storage in the form of cookies).

the GDPR, CCPA, Do Not Call, and other privacy laws and regulations.[46] Consentua and Consentric, both consent managers, make the same type of promises. The former assures customers that its "platform surpasses GDPR requirements."[47] The latter states that it "aligns with existing data privacy regulation," a legal conclusion about its software.[48] Again, these statements may be marketing gimmicks; it is difficult to determine if Consetua's software does indeed go above and beyond the GDPR's rules. But either way, vendors are designing software to meet or exceed their interpretations of legal requirements.

C. Incident Response

Incident response platforms provided by sixty-three vendors can help companies respond to data breaches swiftly and with proper notice,[49] as required by the GDPR[50] and statutes in every state in the United States.[51] There are two types of vendors in this space. Companies like Proofpoint position themselves as technological resources to stay ahead of and respond to digital threats. They don't make promises about regulatory compliance.[52] Other vendors make legal conclusions about their tools and guarantee legal compliance as part of technical incident response. Resilient, for example, states that its Privacy Module guides clients "through the *correct* response to data loss incidents, helping to meet the regulatory deadlines" and other GDPR requirements.[53] It tells clients which authorities to notify, "how they should be notified, and what information is required," and provides their own proprietary templates for those purposes.[54] Radar, which provides data breach incident response management, states that it "generates an incident specific response plan and notification guidelines according to federal, state, and international laws" and "provides all the required documentation to

46 *Compliance and Privacy*, POSSIBLENOW, https://www.possiblenow.com/privacy-compliance.php (last visited Apr. 24, 2021); *see California Consumer Privacy Act (CCPA)*, POSSIBLENOW, https://www.possiblenow.com/california-consumer-privacy-act (last visited Apr. 24, 2021); *Do Not Call Compliance—DNCSolution*, POSSIBLENOW, https://www.possiblenow.com/do-not-call-compliance (last visited Apr. 24, 2021).

47 CONSENTUA, https://consentua.com/ (last visited Apr. 24, 2021).

48 *Consentric*, MYLIFE DIGITAL, https://mylifedigital.co.uk/consent-preference-management/ (last visited Apr. 24, 2021).

49 *See* TECH VENDOR REPORT, *supra* note 11, at 5, 9–10.

50 *See* GDPR, *supra* note 12, art. 33(1) (requiring notification to national data protection authorities within seventy-two hours of a data breach).

51 *See Security Breach Notification Laws*, NAT'L CONF. STATE LEGISLATURES (July 17, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

52 *See* PROOFPOINT, https://www.proofpoint.com/us (last visited Apr. 24, 2021).

53 RESILIENT, BREACH NOTIFICATION UNDER THE GENERAL DATA PROTECTION REGULATION: NEW CAPABILITIES IN THE IBM RESILIENT INCIDENT RESPONSE PLATFORM (2018), https://www.ibm.com/downloads/cas/9WYZP24P (emphasis added).

54 *Id.*

support the organization's burden of proof obligation under the breach laws."[55] To do that, though, Resilient and Radar have to code interpretations of the law into those guidelines, recommendations, and templates.

D. De-Identification Software

Software from forty-six companies purports to allow organizations to process personal data safely in compliance[56] with various state,[57] national,[58] and international statutes[59] that require data anonymity or pseudonymity. But these laws leave room for interpretation: engineers at these vendors decide both the kind of anonymization used and the subset of data to which it applies. Arcad Software, for example, says that its "DOT Anonymizer" is "[d]esigned to meet the strictest requirements of the GDPR" by "hiding or anonymizing the personal elements of data."[60] But that requires coding for what a law defines as "personal elements," a process the company does not explain. Similarly, when Truata claims its service offers its customers a way to meet the GDPR's high anonymity threshold to process, analyze, and "extract value" from anonymized data,[61] it is necessarily translating a legal requirement into coding language.

II. THE IMPLICATIONS OF OUTSOURCING PRIVACY COMPLIANCE

Future research may provide a richer and more detailed picture of the promises and reality of the privacy technology vendor market. Suffice it to

---

55 *Radar Incident Response Management Software*, RADARFIRST, https://www.radarfirst.com/resources/product-info/radar-datasheet/ (last visited Apr. 24, 2021); *see also Simplify Compliance with GDPR Breach Notification Obligations*, RADARFIRST, https://www.radarfirst.com/gdpr (last visited Apr. 24, 2021).

56 *See* TECH VENDOR REPORT, *supra* note 11, at 5, 9.

57 *See, e.g.*, CAL. CIV. CODE § 1798.140(o)(1) (West 2020) (defining "[p]ersonal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household").

58 *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033–34 (codified as amended in 42 U.S.C.); *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1736–38 (2010) (discussing how HIPAA's Privacy Rule was promulgated alongside a strong "faith in the power of anonymization" to protect personal information).

59 The GDPR applies to "personal data," which is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR, *supra* note 12, art. 4(1); *see also id.*, recital 25.

60 ARCAD SOFTWARE, PROTECTION OF PERSONAL DATA, https://www.arcadsoftware.com/resource-items/white-paper-dot-anonymizer/ (last visited Apr. 24, 2021).

61 *See* TECH VENDOR REPORT, *supra* note 11, at 160.

say, however, that at least some of these 259 vendors are including in their technologies their own interpretations of legal requirements. For the most part, the IAPP sees the growth of privacy technology vendors as a good thing: privacy professionals "can now shop among dozens of vendors to find solutions to challenges created" by the GDPR and other laws.[62] The organization has a financial interest in saying that. Many of the IAPP's conferences are sponsored by privacy tech vendors: the IAPP's 2020 Summit Sessions, for example, were principally sponsored by OneTrust Data Discovery, TrustArc, Cisco, BigID, OneTrust Vendorpedia, and WireWheel, all privacy technology vendors on the market.[63] Moreover, the IAPP's comments speak to the advantage of having many market participants, not the value and effectiveness of an industry where engineers make legal conclusions. Indeed, the implications of that kind of outsourcing to technology are troubling. It threatens to amplify the power of the largest technology companies at the expense of their smaller competitors while also narrowing privacy law, undermining expertise, and eroding accountability.[64] This section describes each of those risks in turn.

A. Power Asymmetries

Outsourcing is often cheaper than building something internally, the latter of which requires in-house technical expertise, large salaries and benefits for new hires, and institutional time and capacity.[65] Indeed, as the IAPP and TrustArc recently found, budgetary constraints likely explain why many companies have neither conducted nor hired anyone to help with data mapping, data inventories, or privacy impact assessments despite GDPR requirements.[66]

Even for those companies in the technology vendor market, size, and budget matter. Hiring vendors requires legwork: a clear set of goals, ongoing relationship maintenance, employee training, technology assessment, and integrating the technology into the company practice and routine.[67] Denise Farnsworth, then Jazz Pharmaceuticals CPO, recommended first "go[ing] through the regulations and statutes that are relevant to your company, then you determine the thing you need to comply with" before hiring a vendor.[68]

62 IAPP, 2018 PRIVACY TECH VENDOR REPORT 16 (V.2.4e ed. 2018), https://iapp.org/media/pdf/resource_center/2018TechVendorReport.pdf [hereinafter 2018 TECH VENDOR REPORT].

63 *See IAPP Summit Sessions*, IAPP, https://iapp.org/conference/virtual-sessions/summit-sessions/ (last visited Apr. 24, 2021).

64 This list excludes some obvious risks associated with new technologies, including post-release bugs and failures, that may expose the company to even greater risk.

65 *See* 2018 TECH VENDOR REPORT, *supra* note 62, at 18–19.

66 *See* MEASURING PRIVACY, *supra* note 30, at 4, 7–8, 11 (reporting on results of survey of 496 privacy professionals).

67 *See* 2018 TECH VENDOR REPORT, *supra* note 62, at 16–18.

68 *Id.* at 17.

Anick Fortin-Cousens, then CPO of IBM Canada, noted that vendor management is "a big job for the vendor and for the purchasing company. Implementation involves a lot of back and forth. It's a real partnership and requires assigned resources on the part of the vendor and customer. We had daily and weekly interactions . . . ."[69] And once the vendor's product is up and running, there's more work to be done, including training and integrating the use of the product into the corporate culture.[70] All of that takes time and money, two things that small companies and startups don't have.

Larger companies can leverage internal expertise to conduct extensive due diligence, beta testing, and background research on potential vendors. They can leverage superior bargaining power to adapt vendor products to their interests. They can even buy the best products, leaving the rest of the market with inferior choices or just more expensive ones. And given that these technologies embody legal interpretations, the advantages of size and scale will allow large companies to build structures that frame the law in ways that benefit them, not their competitors and consumers.[71]

B. Narrowing Privacy Law

These concerns alone should give privacy professionals pause. But even more systemic dangers are looming. Outsourcing compliance to technology vendors may narrow and limit privacy protections for users in two different ways. First, translating privacy law into technology platforms reduces privacy law to its codable pieces. Some privacy compliance technologies, therefore, embody an epistemic error: they assume that privacy law is reducible to factors that AI can identify. It isn't.[72] Privacy also involves managing users' expectations, their desire for obscurity,[73] their need for trust,[74] and their

69 *Id.* at 22.

70 *Id.* at 25.

71 *See* Waldman, *Privacy Law's*, *supra* note 8, at 797–98.

72 Scholars recognize that not everything can be coded, especially when it comes to persons and data. *See, e.g.*, Mireille Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 20 THEORETICAL INQUIRIES L. 83, 85 (2019) (recognizing that there are elements of the human self not computable); *see also* BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 29–34 (2018) (arguing that AI solutions to social problems transforms humans into mere "cogs" in the wheel); Benjamin W. Cramer, *To Save Everything, Click Here: The Folly of Technological Solutionism*, 4 J. INFO. POL. 173, 173 (2014) (reviewing EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM (2013) (coining the term "technological solutionism" to describe the approach that everything has an engineering solution)). *See generally* JARON LANIER, YOU ARE NOT A GADGET (2010) (discussing the dehumanizing effects of solely technical solutions).

73 *See* Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1345–46 (2015).

74 *See* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 434 (2016). *See generally* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018) [hereinafter WALDMAN, PRIVACY AS TRUST].

consistent distaste for transfers of data to third parties,[75] not just paper trails and data maps. Even the best technology products cannot capture all of that.

Second, and perhaps more importantly, privacy technology vendors recast the GDPR's focus from reducing privacy risks for the consumer to reducing the risk that the company will face investigation and litigation.[76] ZLTech, for example, markets its "GDPR-Ready Solutions" as ways to avoid "the risk of unprecedented sanctions."[77] And Clarip, a software-as-service provider, bills itself as "the next generation . . . data privacy platform that helps brands minimize privacy risks."[78] Ethyca puts "[d]ata [p]rivacy" and "[r]isk [m]anagement" together and wants to automate privacy "with no loss in efficiency."[79] And the compliance assistance company, 2BAdvice, wants to show its clients how "to save time and money and minimize risk through automating processes."[80] These are just a few examples. Risk avoidance is a trope in the privacy technology vendor market: of the 259 companies profiled in the IAPP's 2019 Privacy Technology Vendor Report, seventy-nine of them describe their risk mitigation work in terms of reducing corporate risk; only four talk about minimizing privacy risks to customers.[81]

Framing the data privacy landscape as one based on corporate risk is not surprising. Some argue that risk framing can actually encourage compliance with the law by persuading executives to treat it as a high priority, especially when some executives still see privacy as inconsistent with corporate profit goals.[82] The risk of a fine of four percent of global revenue under the GDPR could also go a long way to making privacy compliance a central corporate mission.[83] Risk framing also makes sense from an endogenous political perspective. By emphasizing the dangers of noncompliance, privacy professionals stake out important territory at the highest levels of corporate decisionmaking, giving them seats at the table and the capacity to influence policy.[84] This can also encourage third-party vendors seeking corporate contracts to follow suit because it allows them to market themselves as sharing the same values as their corporate clients.

---

75 *See* Kirsten Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, 31 HARV. J.L. & TECH. 111, 131–34 (2017).

76 *See* Waldman, *Privacy Law's*, *supra* note 8, at 798–803.

77 ZLTECH, GDPR-READY SOLUTIONS (on file with author).

78 *Clarip is the Next Generation SaaS Data Privacy Platform that Helps Brands Minimize Privacy Risks and Engage Customers Better*, CLARIP, https://www.clarip.com/business (last visited Apr. 24, 2021).

79 *Our Mission: To Build Trust in the Internet & Data-Driven Business*, ETHYCA, https://ethyca.com/about-ethyca/ (last visited Apr. 24, 2021).

80 *See* 2BADVICE, https://www.2b-advice.com/en/ (last visited Apr. 24, 2021).

81 *See* TECH VENDOR REPORT, *supra* note 11, at 28–172 (data is based on the language this subset of companies included in the Tech Vendor Report).

82 *See* Kaminski, *supra* note 29, at 1603–05 (suggesting that overtime, having to complete assessments and other compliance documents will normalize the process and integrate privacy into everyday work).

83 GDPR, *supra* note 12, arts. 58, 83.

84 *See* EDELMAN, *supra* note 9, at 97–98.

But risk framing is problematic if the goal is adherence to the substantive goals of privacy law. It is incomplete. There is more to privacy than managing risks of a lawsuit. Operating along narrow risk-mitigation paths distracts corporate attention from more important, substantive mandates and focuses employees squarely on their employers' interests. Framing privacy obligations in terms of corporate risk focuses only on the avoidance of a corporate problem rather than the achievement of an affirmative social goal—namely, greater user privacy and safety and limits on the collection and processing of personal data. In a regulatory context where lawsuits are nearly impossible and regulatory oversight is spotty at best, recasting the GDPR's attention to risk undermines the law's ability to effectuate real change in corporate behavior and technology design. So, although a few scholars have suggested that some privacy professionals see the law's requirements as a floor for their work,[85] other social forces on the ground are pulling in the opposite direction.[86]

C. Erosion of Expertise

Outsourcing legal decisions to engineers is a threat to the role of expertise in society. Many technology vendors are coding their interpretations of legal requirements into their products, offering them as solutions to legal problems. That work often happens without lawyers. Advanced Metadata, for example, makes much of its "[twenty] years of experience in data science and information management," but not one of its eight executive team members focuses on regulatory issues.[87] CipherCloud, which provides cloud-based data mapping, hosted a webinar in which its senior vice president of strategy and alliances and its vice president of marketing, neither of whom are privacy professionals or privacy lawyers, claimed that the company's cloud-based tools can help reach GDPR compliance "with [f]our [k]ey [c]apabilities."[88] That is a legal conclusion made by salespersons. Making legal conclusions without legal expertise, and burying those conclusions into code, risks making bad products. Further, it also constitutes a threat to the legal and privacy professions by implicitly characterizing the skills of legal interpretation and implementation as

85 *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 265 (2011).

86 Elsewhere, I explained in more detail how the systems of compliance that CPOs put in place belie any professed interest in going above and beyond the requirements of privacy law. *See generally* Waldman, *Privacy Law's*, *supra* note 8, at 805.

87 *See* ADVANCED METADATA, http://metricsinthemist.com/amd_web/index.html (last visited Apr. 24, 2021).

88 *See Navigate GDPR with Four Key Capabilities*, CIPHERCLOUD, https://www.ciphercloud.com/webinars/why-do-you-need-a-casb-8/ (last visited Apr. 24, 2021).

routinizable, irrational, imperfect, or just too human.[89] As Frank Pasquale has argued, the notion that any engineer, entrepreneur, or businessperson can neatly code privacy law and the human judgments and negotiations it demands, into a machine loses the "[q]ualitative evaluation and . . . humble willingness to recalibrate and risk-adjust quantitative data" that comes with human experts.[90]

D. Lack of Accountability

Privacy technology vendors also change the discourse of power. The language we use shapes our understanding and perceptions of legitimacy, reality, and legality.[91] As Michel Foucault argued, "[d]iscourse transmits and produces power."[92] Critical race theorists have made similar arguments about the power of speech.[93] As have feminist scholars.[94] Our social understanding of privacy is written and discussed in a variety of ways, but through the noise, the discourse is accessible to consumers: "anonymity" protects people from the effects of revelation,[95] we want more "control" over our information,[96] and

89 *See* ADAM GREENFIELD, RADICAL TECHNOLOGIES: THE DESIGN OF EVERYDAY LIFE 190–207 (2017); Frank Pasquale, *A Rule of Persons, Not Machines: The Limits of Legal Automation*, 87 GEO. WASH. L. REV. 1, 19–32 (2019) (challenging the view that contracts and legal provisions can be coded).

90 Frank Pasquale, *Professional Judgment in an Era of Artificial Intelligence and Machine Learning*, BOUNDARY 2, Feb. 2019, at 73, 74.

91 *See* Linda J. Nicholson, *Introduction*, *in* FEMINISM/POSTMODERNISM 1, 11 (Linda J. Nicholson ed., 1990) ("[C]onceptual distinctions, criteria of legitimation, cognitive procedural rules, and so forth are all political and therefore represent moves of power . . . [though] they represent a different type of power than is exhibited in, for example, physical violence or the threat of force.").

92 MICHEL FOUCAULT, THE HISTORY OF SEXUALITY 101 (Robert Hurley trans., 1978); *see also* Gerald Turkel, *Michel Foucault: Law, Power, and Knowledge*, 17 J.L. & SOC'Y 170, 172 (1990) (describing Foucault's argument on "discourses of domination").

93 *See, e.g.*, Charles R. Lawrence III, *If He Hollers Let Him Go: Regulating Racist Speech on Campus*, 1990 DUKE L.J. 431, 444 ("[R]acist speech constructs the social reality that constrains the liberty of non-whites because of their race."); *see also* PATRICIA J. WILLIAMS, THE ALCHEMY OF RACE AND RIGHTS 61 (1991) (arguing that we live with the legacy of slavery in part through "powerful and invisibly reinforcing structures of thought, language, and law").

94 *See, e.g.*, MARGARET THORNTON, DISSONANCE AND DISTRUST: WOMEN IN THE LEGAL PROFESSION (1996) (using real world examples of female lawyers to argue that Foucault's discourse of power is fundamentally a gendered dynamic).

95 This is particularly helpful for members of marginalized and stigmatized communities. *See, e.g.*, Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U.L. REV. 159, 162 (2015) (arguing that privacy should be understood as preventing intimate information from serving as the basis of discrimination).

96 *See* JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 56 (1992) (privacy is "control over a realm of intimacy"); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (defining privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others").

we "trust" our friends to keep our secrets.[97] Shifting that discourse into the language of technology—binary code, source code, "black box" algorithms[98] protected by trade secrecy,[99] emergent and intelligent machines[100]—empowers technologists as the new governors of society and the dictators of social control. This disempowers consumers, who have no access to a technology-driven privacy discourse.

It also undermines the promise of privacy law to hold companies accountable. Privacy technologies embody particular visions of what privacy laws require. But the design process where that instantiation occurs is almost entirely hidden to us. If regulators ever hope to hold technology companies accountable for misusing our data, they will need more than just a vendor contract to do it. As Danielle Citron has argued, the tendency to shift legal decisions to automated technologies erases the safeguards guaranteed by due process, leaving consumers unprotected.[101] The more we ask "black box" algorithms to implement the law, the more we undermine the project of public governance.[102]

---

97 *See* WALDMAN, PRIVACY AS TRUST, *supra* note 74, at 51–52 (noting that trust allows us to share because it creates expectations of confidentiality and adherence to norms).

98 *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 8 (2015).

99 There is a growing literature on the role of trade secrecy in keeping algorithms hidden from users. *See, e.g.*, Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 5 (2014) (algorithms are "shrouded in secrecy"); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1349–53 (2018) (arguing that trade secrecy should not be privileged in criminal proceedings, especially where automated systems are being used to take away liberty). The arguments are being made in court. *See, e.g.*, State v. Loomis, 881 N.W.2d 749, 757 (Wis. 2016).

100 Some scholars note that the discourse of AI is inherently hidden from us. *See, e.g.*, Maayan Perel & Niva Elkin-Koren, *Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement*, 69 FLA. L. REV. 181, 186–90 (2017) (explaining why transparency would not help ordinary users understand automated decision making algorithms); *see also* Julie Brill, Former Comm'r, Fed. Trade Comm'n, Transparency, Trust, and Consumer Protection in a Complex World, Keynote Address Before Coalition for Networked Information 8–9 (Dec. 15, 2015), https://www.ftc.gov/system/files/documents/public_statements/895843/151216cnikeynote.pdf (former FTC Commissioner, Julie Brill, noting difficulties in making algorithms transparent, calling on companies to address fairness themselves).

101 *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U.L. REV. 1249, 1253–56 (2008).

102 *See, e.g.*, Hous. Fed'n of Tchrs. v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1180 (2017) (concluding that the use of a proprietary algorithm to determine teacher hiring, contract renewal, and promotion gave teachers "no meaningful way to ensure correct calculation of their . . . scores, and as a result [we]re unfairly subject to mistaken deprivation of constitutionally protected property interests in their jobs").

CONCLUSION

Companies in the information industry are fond of telling us that our privacy is important to them. And yet, managerializing privacy compliance suggests otherwise. A company that outsources privacy compliance to technology vendors is arguably conceding that privacy is not one of its "core competencies." Core business practices are done in house, not farmed out to automated systems chosen for their efficiency and their capacity to do their work without disrupting productivity and innovation. It is, of course, possible that a company may see privacy outsourcing more like hiring outside counsel than contracting with vendors to, say, cater meetings and lunches. But by choosing code over human expertise, those companies that hire privacy technology vendors are risking privacy compliance that is narrow and incomplete.

Information industry executives can take that risk because our regulatory institutions have ceded their governance responsibilities to regulated entities and chosen managerial values as their lodestars. As Cohen has argued, managerial regulators prefer light regulatory touches, adopt industry discourses about law and innovation, and conceptualize their jobs not as consumer advocates but as facilitators of corporate innovation. Privacy outsourcing is part of a larger problem of public and private governance in informational capitalism, a symptom of a system in which law and technology have been leveraged to entrench corporate power rather than contain it.