VOLUME 130 DECEMBER 2016 NUMBER 2

HARVARD LAW REVIEW FORUM

LAW, PRIVACY & TECHNOLOGY COMMENTARY SERIES

RECODING PRIVACY LAW: REFLECTIONS ON THE FUTURE RELATIONSHIP AMONG LAW, TECHNOLOGY, AND PRIVACY

Urs Gasser[*]

The history of privacy is deeply intertwined with the history of technology. A wealth of scholarly literature tracks and demonstrates how privacy as a normative concept has evolved in light of new information and communication technologies since the early modern period, when face-to-face interactions were challenged by urbanization and the rise of mass communication.[1] In the beginning of the nineteenth century, a combination of societal changes, institutional developments, and technological advancements gave birth to a series of new threats to privacy. At the time, innovative technologies — including telegraph communications and portable cameras — were among the key drivers (interacting with other factors, such as increased literacy rates) that led to growing concerns about privacy protection. These developments also set the stage for Samuel Warren and later-Justice

[*] Professor of Practice, Harvard Law School; Executive Director, Berkman Klein Center for Internet & Society, Harvard University. I thank Ryan Budish, Herbert Burkert, Alba Hancock, Gregory Muren, Alicia Solow-Niederman, David O'Brien, and Alexandra Wood for helpful comments. This Commentary has been inspired by work on the Privacy Tools for Sharing Research Data project, supported by the National Science Foundation under Grant No. 1237235.

[1] *See, e.g.*, COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992); PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995); ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET (2000); DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (5th ed. 2015); DAVID VINCENT, PRIVACY: A SHORT HISTORY (2016); ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U. L. REV. 703 (1990); William L. Prosser, *Privacy [a Legal Analysis]*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 104 (Ferdinand David Schoeman ed., 1984); Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY § 1:1 (Christopher Wolf ed., 2006).

Louis Brandeis's highly influential 1890 article *The Right to Privacy*,[2] which was written, in large part, in response to the combined negative effects of the rise of the "yellow press" and the adaptation of "instantaneous photography" as privacy-invading practices and technologies.[3] Similarly, advancements in information and communication technologies in the twentieth century, combined with other developments such as the rise of the welfare state, challenged existing notions of information privacy and led to renegotiations of the boundaries between the private and public spheres.

The development, adaptation, and use of innovative technologies that enabled and increased the collection and use of personal information later in the twentieth century were also among the key drivers that led to the birth of modern information privacy law in the early 1970s. Starting in the United States and then extending to Europe, the increased use of computers for information processing and storage by government agencies was an important factor that led to the first generation of modern privacy and data protection laws.[4] Anchored in a set of Fair Information Practices,[5] many of these laws were expanded, adjusted, and supplemented over the following decades in light of evolving technologies and changing institutional practices, which — together with other factors — resulted in an ever-growing cascade of privacy concerns. In the 1990s, for instance, the widespread adoption of internet technology as a global information and communication medium and the rise of the database industry led to a wave of legislative and regulatory interventions aimed at dealing with emerging privacy problems. More recent and more ambitious information-privacy reforms, such as the revision of the influential OECD Privacy Guidelines at the international level,[6] the General Data Protection Regulation in

---

[2] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). The article had profound impact on the development of state tort law and privacy-related causes of action. *See, e.g.*, William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 383–86 (1960); *see also* Daniel Solove, *Does Scholarship Really Have an Impact? The Article that Revolutionized Privacy Law*, TEACHPRIVACY (Mar. 30, 2015), https://www.teachprivacy.com/does-scholarship-really-have-an-impact-the-article-that-revolutionized-privacy-law [https://perma.cc/FB4J-XXKA] (describing *The Right to Privacy* as "one of the most influential law articles" of all time).

[3] *See* Andreas Busch, *Privacy, Technology, and Regulation: Why One Size Is Unlikely to Fit All*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 303, 305 (Beate Roessler & Dorota Mokrosinska eds., 2015).

[4] *See* SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS, at viii–xi (1973).

[5] In essence, Fair Information Practices "are a set of internationally recognized practices for addressing the privacy of information about individuals." Robert Gellman, Fair Information Practices: A Basic History 1 (June 17, 2016) (unpublished manuscript), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf [https://perma.cc/WY5U-RC9A].

[6] ORG. FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980),

the EU,[7] and the proposed Consumer Privacy Bill of Rights Act in the United States,[8] seek to update existing privacy norms for the digital age — again driven, in part, by new technologies and applications such as cloud computing and Big Data, among others.

Reflecting across centuries and geographies, one common thread emerges: advancements in information and communication technologies have largely been perceived as *threats* to privacy and often led policymakers to seek, and consumers to demand, additional privacy safeguards in the legal and regulatory arenas. This perspective on technology as a challenge to existing notions of, and safeguards for, information privacy is also reflective of the mindset of contemporary law and policymaking. Whether considering the implications of Big Data technologies, sensor networks and the Internet of Things, facial recognition technology, always-on wearable technologies with voice and video interfaces, virtual and augmented reality, or artificial intelligence, recent policy reports and regulatory analyses have identified privacy challenges as among the most pressing concerns.[9]

In considering this fundamentally defensive stance that privacy law has taken historically with regard to technology, it is important to note that law in the broader context of information and communication technology often transcends its traditional role as a constraint on behavior acting through the imposition of sanctions. In areas such as intellectual property and antitrust, law seeks to engage with technology in a more nuanced way by *enabling* or in some cases *leveling* desired innovative or disruptive activity.[10] With this understanding of law as a functionally differentiated response system, and an acknowledgment that legal responses to technological innovation should not be understood as a simple stimulus-response mechanism, it is possible to identify a series of *response patterns* when examining the evolution of privacy law vis-à-vis technological change. At a general level, three

---

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/2A69-STS4].

[7] Commission Regulation 2016/679, 2016 O.J. (L 119) 1.

[8] WHITE HOUSE, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT (2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [https://perma.cc/6SY5-VGYF].

[9] *See, e.g.*, EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [https://perma.cc/A7Y9-QUGS]; FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/6D8N-G4AU].

[10] *See* Urs Gasser, *Perspectives on the Future of Digital Privacy*, 134 ZSR II 335, 368–69 (2015). On the innovation-enabling function of law, see also Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639 (2014).

analytically distinct, but in practice often overlapping, response modes can be identified.[11]

(1) When dealing with innovative technologies, the legal system — including privacy law — by default seeks to apply the old rules to the (new) problem resulting from the new technology and its uses (subsumption). U.S. courts' application of privacy torts, for instance, when addressing complaints about improper collection, use, or disclosure by digital businesses such as Google and Facebook — largely relying on tort conceptions of privacy advanced in the late nineteenth century — is an illustration of this default response mode.[12]

(2) Where subsumption is considered insufficient given the novelty of issues raised by a new technology, the legal system might resort to innovation within its own system. One version of this response mode is to "upgrade" existing (privacy) norms gradually, typically by setting new precedent or by adjusting or complementing current norms (gradual innovation). Proposals to introduce a tort for the misuse of personal information by data traders,[13] to provide legal recognition of data harms by extending developments from other areas of the law such as torts and contracts,[14] and to enact a Consumer Privacy Bill of Rights Act,[15] are examples of gradual legal innovations that leave core elements of the current regulatory approach unchanged.

(3) A more radical, paradigm-shifting approach is more deeply layered law reform where not only individual norms are updated but also entire approaches or instruments are changed. Examples in this category include proposals to reimagine privacy regimes based on models that emerged in the field of environmental law,[16] to create an alternative dispute resolution scheme such as a "cyber court" system to deal with large-scale privacy threats in the digital age,[17] or to introduce a "Digital Millennium Privacy Act" that would provide immunity for those companies willing to subscribe to a set of information fiduciary duties,[18] to name just three illustrations.

---

[11] *See* Gasser, *supra* note 10, at 368–69.

[12] *See, e.g.*, Boring v. Google Inc., 362 Fed. App'x 273, 278–80 (3d Cir. 2010).

[13] *See* Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 173 (2006).

[14] *See* Daniel J. Solove & Danielle Keats Citron, Privacy and Data Security Harms 41 (unpublished manuscript) (on file with the Harvard Law School Library).

[15] *See* WHITE HOUSE, *supra* note 8.

[16] *See* Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1 (2006).

[17] *See* Lucille M. Ponte, *The Michigan Cyber Court: A Bold Experiment in the Development of the First Public Virtual Courthouse*, 4 N.C. J.L. & TECH. 51 (2002).

[18] Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, THE ATLANTIC (Oct. 3, 2016), http://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346 [https://perma.cc/NX5E-2653].

Perhaps the most interesting, and arguably the most promising, approach to reprogramming privacy law in a more fundamental sense is linked to a potential paradigm shift: embracing the multifaceted, functional role of law and reframing technology, broadly defined, no longer (only) as a threat to privacy, but as part of the *solution space*. Precursors of such a potential shift date back to the 1970s, when researchers started to develop technical mechanisms under the header of "Privacy-Enhancing Technologies" (PETs) in response to privacy challenges associated with new information and communication technologies.[19] Originally focused on identity protection and technical means to minimize data collection and processing without losing a system's functionality, the scope of PETs and the available instruments have broadened over time to include encryption tools, privacy-preserving analysis techniques, data management tools, and other techniques covering the entire lifecycle of personal data. Starting in the 1990s, PETs as one instrument in the toolbox were put into a larger context by the introduction of Privacy by Design as a "systematic approach to designing any technology that embeds privacy into the underlying specification or architecture."[20] Still remaining a somewhat amorphous approach, Privacy by Design as an umbrella philosophy (as well as certain types of PETs) promotes a means to manage privacy challenges resulting from a wide range of emerging technologies, and has been adopted by law and policymakers on both sides of the Atlantic, with the EU General Data Protection Regulation among the most prominent examples.[21]

Law's relatively recent "discovery" of technology as an approach to address the very privacy challenges technology (co-)creates has potential. The approach's promise manifests itself not so much at the mechanical level of individual techniques and tools. Rather, it becomes visible when considering the types of *perspectives* an approach situated at the law/technology interface opens up when dealing with the privacy challenges of the digital age. Projecting from the past into the future, approaches like Privacy by Design signal a departure from binary notions of privacy and ad hoc balancing tests of competing interests toward more holistic and rigorous *privacy risk assessment* models that rely on modeling approaches from information security and an understanding of privacy that is informed by recent theoretical advances across different disciplines. A growing body of interdisciplinary research demonstrates the theoretical and practical promise of holistic

---

[19] *See* HANDBOOK OF PRIVACY AND PRIVACY-ENHANCING TECHNOLOGIES: THE CASE OF INTELLIGENT SOFTWARE AGENTS (G.W. van Blarkom, J.J. Borking & J.G.E. Olk eds., 2003).

[20] Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1411–12 (2011).

[21] *See* Commission Regulation 2016/679, *supra* note 7, at art. 25.

analytical frameworks for a modern privacy analysis that incorporates recent research from fields such as computer science, statistics, law, and the social sciences.[22] This promise does not mean that a blended approach has no issues; to the contrary, there are significant limitations including, among others, internal constraints, incentive misalignments, and broader normative challenges. Yet these challenges are properly understood as issues of operationalization and ought not automatically foreclose a reconceptualization of the relevant solution space.

In addition to advancing new *tactical* methods to conceptualize and evaluate privacy risk, embedding technology into (privacy) law can boost the development of new solutions to *more strategically manage* a broad range of privacy risks. Research initiatives across the country show how emerging technical privacy solutions, including sophisticated tools for data storage and access control, as well as advanced tools for data analysis and release, can play in concert with legal, organizational, and other safeguards to manage privacy risks across the different stages of the lifecycle of data.[23] Consider, for instance, the important role encryption plays in securing access to and storage of data,[24] or the technological development of a personal data store that enables individuals to exercise fine-grained control over where information about them is stored and how it is accessed.[25] Differential privacy is a new formal mathematical framework for addressing privacy challenges associated with the statistical analysis of information maintained in databases.[26] Secure multiparty computation, to add another example, is a method that enables parties to carry out a joint computation over their data in such a way that no single entity needs to hand a dataset to any other explicitly.[27] While some of these technologies are still in development, others have been tested out in practice and are already recommended as best practices in selected fields of application.

---

[22] For examples from research that illustrate the benefits of such a blended approach, see Micah Altman et al., *Towards a Modern Approach to Privacy-Aware Government Data Releases*, 30 BERKELEY TECH. L.J. 1967 (2015); and Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703 (2016).

[23] *See, e.g.*, *Privacy Tools for Sharing Research Data*, HARV. UNIV. PRIVACY TOOLS PROJECT, http://privacytools.seas.harvard.edu/project-description [https://perma.cc/BCU6-AMJL] (supported by NSF grant CNS-1237253).

[24] For a description of encryption standards for federal government information systems, see, for example, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, FIPS PUB. 140-2: SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES (2001), http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf [https://perma.cc/95QV-6ZAL].

[25] *See* Tom Kirkham et al., *The Personal Data Store Approach to Personal Data Security*, IEEE SECURITY & PRIVACY, Sept./Oct. 2013, at 12, 13.

[26] *See* Cynthia Dwork, *Differential Privacy*, *in* ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY 338 (Henk C.A. van Tilborg & Sushil Jajodia eds., 2d ed. 2011).

[27] *See* Yehuda Lindell & Benny Pinkas, *Secure Multiparty Computation for Privacy-Preserving Data Mining*, 1 J. PRIVACY & CONFIDENTIALITY 59, 60 (2009).

In the digitally networked world, the regulation of information privacy has an inherently technical dimension. Such technological aspects have been the focus of intense study by computer scientists, resulting in a rich theoretical literature as well as practical tools for protecting privacy, but such discussion has by and large occurred in a space separate from the sphere of legal norms, regulations, policies, ethics codes, and best practices. A number of trends make it important and urgent to overcome the silos that have been created, to foster knowledge sharing between the two spheres, and to embrace technological approaches to support legal privacy across the different functions mentioned before.

Technological advances, for instance, are enabling new and sophisticated attacks that were unforeseen at the time that legal standards for privacy protection were drafted. Computer scientists have developed approaches that are robust not only against known modes of attack, but also against unknown future attacks, and are therefore well suited to address challenges posed by new technological threats to privacy.

Further, legal standards can result in wide variations in treatment of data across contexts, depending on the jurisdictions, industry sectors, actors, and categories of information involved. New frameworks for evaluating privacy threats based on both legal and scientific standards for privacy protection could be used to provide more comprehensive, consistent, and robust data privacy protection, thereby furthering end goals of the law.

Finally, traditional legal approaches for protecting privacy while transferring data, making data-release decisions, and drafting data-sharing agreements, among other activities, are time-intensive and not readily scalable to Big Data contexts. Technological approaches can be designed with compliance with legal standards and practices in mind, in order to help automate data-sharing decisions and ensure consistent privacy protection at a massive scale.

These and related examples indicate how law and technology can advance the state of the practice through a *mutually productive relationship*. Taken together, the development of privacy tools that aim to *integrate* legal and technical approaches could help pave the way for a more strategic and systematic way to conceptualize and orchestrate the contemporary interplay between law and technology in the field of information privacy. In concrete terms, this path could urge actors to incorporate modern legal and technological approaches in their privacy analysis frameworks and to adopt tiered-access models that integrate both legal and technical tools for privacy protection.[28] When

[28] *See, e.g.*, Altman et al., *supra* note 22.

demonstrating a privacy technology's compliance with legal standards for privacy protection, policymakers and technologists could seek to employ a hybrid of legal *and* technical reasoning.[29] And regulatory systems and institutions could support additional research on policy reasoning, accountable systems, and computable policies for automating compliance with legal requirements and enforcement of privacy policies.[30] Such integrated approaches recognize the rich roles that law can play alongside the technical space and hint at how more robust and effective privacy protections can emerge by melding different instruments and methods — both at the conceptual and implementation levels.

These developments might ultimately culminate in a more deeply layered *recoding* of privacy law that leverages the synergies between technological and legal perspectives and instruments and transcends the traditional response patterns discussed earlier in this Commentary in order to cope with the complex privacy-relevant challenges of our future. For example, in light of substantial definitional gaps between various technological and legal approaches to privacy, updating the law to better support new privacy technologies could require a fundamental reframing away from traditional legal notions such as "Personally Identifiable Information"[31] and "de-identification."[32] Furthermore, legal standards could be redesigned to focus on the ends rather than the means of privacy protection, which are likely to continue to evolve rapidly. Rather than implicitly or explicitly endorsing traditional approaches like de-identification, updated legal standards might, for instance, adopt more general descriptions of the intended privacy goal, which would provide a clearer basis for demonstrating whether new classes of emerging privacy technologies are sufficient.

However, such a strategy requires significant investments in interdisciplinary education, research, and collaboration.[33] Programs de-

---

[29] *See* Kobbi Nissim et al., Bridging the Gap Between Computer Science and Legal Approaches to Privacy (June 8, 2016) (unpublished manuscript), http://privacytools.seas.harvard.edu/files/privacytools/files/bridging_cs_law_privacy.pdf [https://perma.cc/A8LU-YAN7].

[30] *See, e.g.*, DANIEL J. WEITZNER ET AL., COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY TECHNICAL REPORT: INFORMATION ACCOUNTABILITY (2007); Henry DeYoung et al., *Experiences in the Logical Specification of the HIPAA and GLBA Privacy Laws*, *in* PROCEEDINGS OF THE 9TH ANNUAL ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY 73 (2010); Lalana Kagal & Joseph Pato, *Preserving Privacy Based on Semantic Policy Tools*, IEEE SECURITY & PRIVACY, July/Aug. 2010, at 25.

[31] *See, e.g.*, Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1816 (2011).

[32] *See, e.g.*, SIMSON L. GARFINKEL, NAT'L INST. OF STANDARDS & TECH., DEP'T OF COMMERCE, DE-IDENTIFICATION OF PERSONAL INFORMATION (2015), http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf [https://perma.cc/ZPY7-KCX4].

[33] *See, e.g.*, NAT'L SCI. & TECH. COUNCIL, NATIONAL PRIVACY RESEARCH STRATEGY (2016), https://www.whitehouse.gov/sites/default/files/nprs_nstc_review_final.pdf [https://perma.cc/SXJ4-3WTD].

signed to stimulate collaboration and interdisciplinary learning have been developed at universities.[34] Furthermore, technology positions in government, such as the Chief Technologist position at the Federal Trade Commission, and advisory panels such as the President's Council of Advisors on Science and Technology, recognize the need for experts in computer science to inform the regulation of privacy and to serve as promising examples of cross-disciplinary communication and knowledge sharing in policy circles.[35] Similarly, it is becoming increasingly important for technologists to understand legal and policy approaches to privacy protection so that they can implement measures that advance the specific goals of legal and regulatory privacy standards. Doing so will likely require policymakers to develop mechanisms and resources for communicating their shared understanding of the interface between law and technology to privacy practitioners. There is much yet to be uncovered: development of novel systems of governance requires not only interdisciplinary mutual understandings, but also deep inquiry into the most effective role for law and legal governance in such a dynamic, fast-changing system.

Reimagining the relationship between technology and privacy law in the digital age should be seen as a key component of a larger effort aimed at addressing the current digital privacy crisis more holistically. Under contemporary conditions of complexity and uncertainty, the solution space for the multifaceted privacy challenges of our time needs to do more than treat the symptoms of discrete privacy ills. It needs to combine approaches, strategies, and instruments that span all available modes of regulation in the digital space, including technology, markets, social norms, and the law. If pursued diligently and collaboratively, such a turn toward *privacy governance* could result in a future-oriented privacy framework that spans a broad set of norms, control

---

[34] Examples in the field of research are initiatives such as the Privacy Tools for Sharing Research Data at Harvard University, which brings together computer scientists, statisticians, legal scholars, and social scientists to tackle difficult problems at the intersection of privacy and technology, or the efforts by the Center on Privacy & Technology at Georgetown University Law Center, which aims to build interdisciplinary bridges between law and computer science thinking with respect to privacy. Interdisciplinary courses in privacy at Princeton, CMU, MIT, and Harvard serve as possible sources of inspiration in the educational realm. *See, e.g.*, ARVIND NARAYANAN, PRINCETON UNIV., PRIVACY TECHNOLOGIES: AN ANNOTATED SYLLABUS, http://randomwalker.info/publications/privacyseminar.pdf [https://perma.cc/8YZE-NP9K]; *8-533/8-733/19-608/95-818: Privacy Policy, Law, and Technology*, CARNEGIE MELLON U., https://cups.cs.cmu.edu/courses/pplt-fa16 [https://perma.cc/HW92-DZ8H]; *6.S978 Privacy Legislation: Law and Technology (2-3-7)*, MASS. INST. OF TECH., https://groups.csail.mit.edu/mac/classes/6.S978 [https://perma.cc/VKP9-FPH7]; *Comparative Online Privacy*, HARV. L. SCH., http://hls.harvard.edu/academics/curriculum/catalog/default.aspx?o=69463 [https://perma.cc/BH8D-BP98].

[35] *See* Latanya Sweeney, *Technology Science*, FTC: TECH@FTC (May 2, 2014, 11:02 AM), https://www.ftc.gov/news-events/blogs/techftc/2014/05/technology-science [https://perma.cc/A88J-DAHE].

mechanisms, and actors — "a *system* of information privacy protection that is much larger, more complex and varied, and likely more effective, than individual information privacy rights."[36] Through such nuanced intervention, the legal system (understood as more than merely a body of constraining laws) can more proactively play a key role in coordinating the various elements and actors in the new governance regime, and — above all — in ensuring the transparency, accountability, and legitimacy that allow democratic governance to flourish.

[36] Viktor Mayer-Schönberger, *Beyond Privacy, Beyond Rights — Toward a "Systems" Theory of Information Governance*, 98 CALIF. L. REV. 1853, 1883 (2010).