9

Futuring Digital Privacy

Reimaging the Law/Tech Interplay

*Urs Gasser**

A INTRODUCTION

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 – such as 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 Louis Brandeis's highly influential

* Urs Gasser is Professor of Practice and Executive Director of the Berkman Klein Center for Internet and Society, Harvard Law School. Contact: ugasser@law.harvard.edu.

[1] See, e.g., C. J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992); P. M. Regan, *Legislating Privacy: Technology, Social Values, and Curiosity from Plymouth Rock to the Internet* (Chapel Hill: The University of North Carolina Press, 1995); R. E. Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* (Providence: Privacy Journal, 2000); D. J. Solove and P. M. Schwartz, *Information Privacy Law*, 5th edn (New York: Wolters Kluwer 2015); D. J. Solove, 'The Origins and Growth of Information Privacy Law', in J. B. Kennedy, P. M. Schwartz, and F. Gilbert (eds), *Fourth Annual Institute on Privacy Law: Protecting Your Client in a Security-Conscious World* (New York: Practising Law Institute, 2003), 29–83; D. Vincent, *Privacy: A Short History* (Cambridge: Polity Press, 2016); A. F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967); I. R. Kramer, 'The Birth of Privacy Law: A Century Since Warren and Brandeis', *Catholic University Law Review* 39 (1990), 703–724; W. L. Prosser, 'Privacy [a Legal Analysis]', in F. D. Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984), 104–155; D. J. Solove, 'A Brief History of Information Privacy Law', in C. Wolf (ed), *Proskauer on Privacy* (New York: Practising Law Institute, 2006), 1–46.

https://doi.org/10.1017/9781108919234.013 Published online by Cambridge University Press

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.

Later in the twentieth century, the development, adaptation, and use of innovative technologies that enabled increased collection and use of personal information 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 information 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 (GDPR) in the EU,[7] the proposed Consumer Privacy Bill of

[2] S. D. Warren and L. D. Brandeis, 'The Right to Privacy', *Harvard Law Review* 4 (1890), 193–220. The article had a profound impact on the development of state tort law and privacy-related causes of action. See, e.g., W. L. Prosser, 'Privacy', *California Law Review* 48 (1960), 386–423; see also D. Solove, 'Does Scholarship Really Have an Impact? The Article that Revolutionized Privacy Law', TeachPrivacy, 30 March 2015.

[3] See A. Busch, 'Privacy, Technology, and Regulation: Why One Size Is Unlikely to Fit All', in B. Roessler and D. Mokrosinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge: Cambridge University Press, 2015), 303–323.

[4] See US Department of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Cambridge, MA: MIT Press, 1973).

[5] In essence, Fair Information Principles 'are a set of internationally recognized practices for addressing the privacy of information about individuals'. R. Gellman, 'Fair Information Practices: A Basic History', unpublished manuscript, 17 June 2016, available at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[6] OECD, *The OECD Privacy Framework: Supplementary Explanatory Memorandum to the Revised OECD Privacy Guidelines* (Paris: OECD, 2013).

[7] Regulation 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), OJ L [2016] 119/1.

Rights Act,[8] or the California Consumer Privacy Act[9] in the United States seek to update existing or introduce new information privacy norms for the digital age – again driven, in part, by new technologies and applications such as cloud computing, big data, and artificial intelligence, 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 have often led policymakers to seek, and citizens 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 (IoT), facial recognition technology, always-on wearable technologies with voice and video interfaces, virtual and augmented reality, or artificial intelligence (AI), information privacy and data protection challenges have surfaced among the most pressing concerns in recent policy reports and regulatory analyses.[10]

But over the decades, the development and adoption of new technologies across varying socio-economic contexts has periodically culminated in critical inflection points that offered individuals and society opportunities to re-examine and advance the notion of privacy itself.[11] Arguably, the current wave of privacy-invasive technologies marks another such inflection point. The scale and pace of society's digital transformation suggest that what is unfolding are not just gradual technological changes, but rather seismic shifts in the information ecosystem that call for a deeper rethinking of privacy.[12] The magnitude of this historical moment is reflected in an array of trends: the rise of data colonialism[13] and surveillance capitalism,[14] increased

[8] The White House, Administration Discussion Draft: Consumer Privacy Bill of Rights Act, 2015, available at https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[9] State of California Department of Justice, California Consumer Privacy Act (CCPA), 2020, available at https://oag.ca.gov/privacy/ccpa.

[10] See, e.g., Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (Washington, DC: The White House, 2014); US Federal Trade Commission, *Internet of Things: Privacy and Security in a Connected World* (Washington, DC: Federal Trade Commission, 2015); Independent High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI* (Brussels: The European Commission, 2019); OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, 21 May 2019.

[11] See, e.g., S. Rodotà, 'Data Protection as a Fundamental Right', in S. Gutwirth et al. (eds), *Reinventing Data Protection?* (New York: Springer, 2009).

[12] W. Hartzog and N. M. Richards, 'Privacy's Constitutional Moment and the Limits of Data Protection', *Boston College Law Review* 61 (2020), 1687–1761.

[13] N. Couldry and U. A. Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford: Stanford University Press, 2019).

[14] S. Zuboff, *Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Hachette Book Group, 2019).

privacy-awareness post Facebook's Cambridge Analytica scandal,[15] AI's ability to amplify privacy risks,[16] and many more.

Some current developments already indicate or suggest shifts and innovations within privacy and data protection regimes in response to the latest changes in the socio-technological environment. For example, basic ideas of how privacy should be defined have already begun to change. At a fundamental level, for instance, some scholars propose to (re-)conceptualize privacy as trust.[17] At a more granular level, scholars have argued for a movement away from understanding privacy as attached to the individual towards a notion of group privacy.[18] In the context of genomics, for example, this idea is particularly important – the exposure of one individual's DNA data directly impacts the privacy rights of that individual's entire extended family. Similarly, privacy risks are no longer generated only by exposure of private data; rather, they can also be triggered by inferences made through analytics.[19] Thus, privacy advocates have called for regulation that protects individuals in not only the inputs but also outputs of data processing.[20]

As legal and regulatory frameworks gradually adapt to these and other facets of privacy, data-holding entities also face the challenge of figuring out the precise contours of their responsibilities to the individuals whose data they collect and process. The development of new accountability frameworks, for instance in the context of data-processing algorithms, as well as novel mechanisms to delineate the responsibilities of these entities, such as the idea of information fiduciaries,[21] also signal a potential paradigm shift in the ways information privacy and data protection are approached.

This chapter is interested in one specific cross-cutting dimension of what might be labelled as the *rethinking privacy discourse*. It asks whether and how the interplay between technology and privacy law – both systems that govern information flows – can be reimagined and organized in mutually productive ways. The chapter proceeds in four steps: (i) explaining some of the dynamics that motivate a rethinking of privacy in the modern moment; (ii) developing a historical understanding of the dominant patterns connecting the evolutions of law and technology; (iii) examining

[15] I. Lapowsky, 'How Cambridge Analytica Sparked the Great Privacy Awakening', *Wired*, 17 March 2019.

[16] K. Manheim and L. Kaplan, 'Artificial Intelligence: Risks to Privacy and Democracy', *Yale Journal of Law and Technology* 21 (2019), 106–188.

[17] See, e.g., A. E. Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge: University Printing House, 2018).

[18] B. Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics', *Philosophy and Technology* 30 (2017), 475–494.

[19] S. Wachter and B. Mittelstadt, 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI', *Oxford Business Law Blog*, 9 October 2018.

[20] Ibid.

[21] J. M. Balkin, 'Information Fiduciaries and the First Amendment', *UC Davis Law Review* 49 (2016), 1183–1234.

a potential way to reimagine the dynamic between these elements moving forward; and (iv) sketching elements of a pathway towards 're-coding' privacy law.

B THE MODERN MOMENT IN TECHNOLOGY

The culmination of multiple factors at the intersection among digital technologies, market paradigms, social norms, professional practices, and traditional privacy laws has prompted the urgency of the need to rethink privacy and data protection in the current moment. Among the most important drivers behind the intensified debates about the future of digital privacy as broadly defined are increasingly visible shifts in traditional power structures, more specifically towards governments with unprecedented surveillance capabilities as well as large technology companies that amass digital tracking technologies and large pools of data to develop the corresponding analytical capability to shape people's lives.[22]

From a historical perspective, it is worth remembering that it was also power shifts that triggered the emergence of the modern information privacy and data protection laws in the 1970s, when the adoption of new technologies in the form of mainframe computers created an imbalance in power between different branches of government.[23] Somewhat similarly, contemporary power struggles among governments, technology companies, and citizens/users might mark another milestone with the potential to affect the political economy of privacy in the longer term. In the United States, the significance of these changes are reflected in a backlash: a variety of developments, ranging from increased activity among lawmakers and regulators[24] to critique by leaders of tech companies themselves,[25] suggest that the 'data-industrial complex' (understood traditionally as the symbiosis between the technology companies of Silicon Valley and the US government) has eroded in the aftermath of the Snowden revelations and in light of the Facebook/Cambridge Analytica scandal, which have demonstrated how profound the effects of such power shifts can be. The ensuing flurry of proposals for privacy legislation at the local, state, and national

[22] Similar shifts triggered a 'rethinking' exercise about a decade ago; see H. Burkert, 'Towards Next Generation of Data Protection Legislation', in S. Gutwirth et al. (eds), *Reinventing Data Protection?* (New York: Springer, 2009).

[23] H. Burkert, 'Theories of Information in Law', *Journal of Law and Information Science* 1 (1982), 120–130.

[24] See, e.g., K. Chen, 'Yanging and Hanging onto Our Own Data', *Berkeley Technology Law Journal Blog*, 30 December 2019; M. Cantwell, 'Cantwell, Senate Democrats Unveil Strong Online Privacy Rights', *Press Release*, 26 November 2019, available at www.cantwell.senate.gov/news/press-releases/cantwell-senate-democrats-unveil-strong-online-privacy-rights; 'Senator Wicker Circulates Draft Privacy Bill', *Hunton Andrews Kurth*, 3 December 2019, available at www.huntonprivacyblog.com/2019/12/03/senator-wicker-circulates-draft-privacy-bill/; D. Shepardson, 'Trump Administration Working on Consumer Data Privacy Policy', *Reuters*, 27 July 2018.

[25] N. Lomas, 'Apple's Tim Cook Makes Blistering Attack on the "Data Industrial Complex"', *TechCrunch*, 24 October 2018.

https://doi.org/10.1017/9781108919234.013 Published online by Cambridge University Press

levels can be understood as attempts to course-correct and address some of the previously less visible power shifts between public and private actors.[26]

Different manifestations and perceptions of such power shifts also fuel international and regional debates that point out the urgent need to address the privacy crisis of the digital age. This crisis has inspired the enactment of the GDPR in Europe and similar legislative efforts in other parts of the world,[27] as well as intensified global debates about 'data sovereignty', which can be understood as an immune system response triggered by the power shifts associated with the unprecedented surveillance capabilities of foreign governments and technology companies.[28]

In addition to tectonic power shifts, technology-induced changes also motivate the need to rethink privacy from within the field. A series of conceptual and definitional questions are illustrative in this respect. For example, is 'personally identifiable information' in a big data environment still a meaningful classification to trigger privacy laws?[29] What about the traditional privacy-protecting techniques, such as anonymization? In a world where volumes of ostensibly innocuous data are available on most individuals, composition effects make re-identification of individuals and reconstruction of databases possible, and even likely, in many cases.[30] How should privacy harms be defined when traditional legal standards do not easily apply to the new types of cumulative, often long-term, and immaterial effects of privacy invasions?[31] These examples are indicative of the need to revisit some of the conventional terms and concepts privacy laws have long relied upon now that they are challenged by technological advances and the socio-economic practices they enable.

Finally, in an increasingly digitally connected environment, privacy has become a complex right that requires re-evaluating the trade-offs inherent to the idea of 'privacy'. Privacy is, of course, not an absolute right; there are limits, barriers, and frequently values that are in tension with each other. Although a concept deeply

[26] See, e.g., 'US 50-State Statutory and Legislative Charts', *IAPP*, available at https://iapp.org/resources/article/us-50-state-statutory-and-legislative-charts/.

[27] See, e.g., 'Data Protection Laws of the World: Full Handbook', *IAPP*, 6 March 2019, available at https://iapp.org/media/pdf/resource_center/Data-Protection-Full.pdf.

[28] See, e.g., S. Couture and S. Toupin, 'What Does the Concept of "Sovereignty" Mean in Digital, Network, and Technological Sovereignty?', *GigaNet Annual Symposium*, 2017.

[29] See, e.g., P. M. Schwartz and D. J. Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information', *New York University Law Review* 86 (2011), 1814–1894; E. Ramirez, 'Protecting Consumer Privacy in the Digital Age: Reaffirming the Role of Consumer Control', Keynote Address of FTC Chairwoman Edith Ramirez Technology Policy Institute Aspen Forum, Aspen, 22 August 2016.

[30] See, e.g., C. Dwork et al., 'Exposed! A Survey of Attacks on Private Data', *Annual Review of Statistics and Its Application*, 2017, 61–84; A. Fluitt et al., 'Data Protection's Composition Problem', *European Data Protection Law Review* 5 (2019), 285–292, at 285–286.

[31] See D. J. Solove and D. Citron, 'Risk and Anxiety: A Theory of Data Breach Harms', *Texas Law Review* 96 (2018), 737–786, at 745–746; 'In re U.S. Office of Personnel Management Data Security Breach Litigation', *Harvard Law Review* 133 (2020), 1095–1102.

shaped by technology, it is also directly linked to shifting social norms and normative expectations.[32] In the age of big data, the balancing act of navigating trade-offs between normative values becomes increasingly important and difficult. For example, the right to be forgotten, by prioritizing privacy interests, necessarily reduces freedom of expression and commercial interests in the data market.[33] The real challenge of privacy has now become figuring out how to balance trade-offs in a scalable manner – whether that requires developing decision trees or balancing tests – that is not merely a post hoc rationalization for a particular outcome. As the design and processes of modern technology become more sophisticated, and as big societal challenges, such as climate change or public health, increasingly rely on the collection and analysis of large amounts of data, these trade-offs will only become more pervasive and more difficult.[34]

Taken together, the modern era of digital technology has arguably pushed the need to rethink 'privacy' to become something more fundamental – a need to re-examine and potentially renegotiate the very concepts and values that society cares about in privacy. Both in terms of problem description and possible pathways forward, this may require, for example, reaching outside the frame of privacy and data protection law altogether to other areas of law and policy writ large. The interplay between technology and society and law is extraordinarily nuanced, and there are a wide variety of levellers and instruments available to help shape the societal effects of technologies in the human context.[35] More narrowly, and simplifying for the purposes of this chapter, it might be helpful to examine some archetypical response patterns from when law has responded to technology-induced information privacy concerns in the past.

C HISTORICAL PATTERNS OF INTERACTION BETWEEN LAW AND TECHNOLOGY

In considering the 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 has often transcended its

[32] K. Nissim and A. Wood, 'Is Privacy Privacy?', *Philosophical Transactions of the Royal Society* A 376 (2018), 1–19.

[33] 'Tradeoffs in the Right to Be Forgotten', *Harvard Civil Rights–Civil Liberties Law Review*, 26 February 2012, available at https://harvardcrcl.org/tradeoffs-in-the-right-to-be-forgotten/.

[34] See, e.g., I. Graef and J. Prüfer, 'Mandated Data Sharing Is a Necessity in Specific Sectors', *Economomisch Statistische Berichten* 103 (2018), 298–301; C. L. Borgman, 'The Conundrum of Sharing Research Data', *Journal of the American Society for Information Science and Technology* 63 (2012), 1059–1078.

[35] See generally Y. Benkler, 'The Role of Technology in Political Economy: Part I', *Law and Political Economy*, 25 July 2018, available at https://lpeblog.org/2018/07/25/the-role-of-technology-in-political-economy-part-1/; Y. Benkler, 'The Role of Technology in Political Economy: Part II', *Law and Political Economy*, 26 July 2018, available at https://lpeblog.org/2018/07/26/the-role-of-technology-in-political-economy-part-2/; Y. Benkler, 'The Role of Technology in Political Economy: Part 3', *Law and Political Economy*, 27 July 2018, available at https://lpeblog.org/2018/07/27/the-role-of-technology-in-political-economy-part-3/.

familiar role as a constraint on behaviour acting through the imposition of sanctions.[36] In areas, such as intellectual property and antitrust, law has sought to engage with technology in a more nuanced way by enabling or in some cases levelling desired innovative or disruptive activity.[37] With this understanding of law as a functionally differentiated response system, and acknowledging that legal responses to technological innovation should not be understood as a simple stimulus-response mechanism, it is possible to identify a series of historical *response patterns* that characterize the evolution of privacy and data protection law vis-à-vis technological change. At a general level, three analytically distinct, but in practice often overlapping, response modes can be identified.[38]

1. When dealing with innovative technologies, the legal system – including privacy and data protection law – by default often seeks to apply the old rules to the (new) problem resulting from new technology and its uses (subsumption). One illustration of this default response mode is US courts' application of privacy torts, for instance, to address complaints about improper collection, use, or disclosure of data by digital businesses, such as Google and Facebook, because these analyses largely rely on tort conceptions of privacy advanced in the late nineteenth century.[39]
2. Where subsumption is considered insufficient due to the novelty of the issues raised by a new technology, the legal system might resort instead 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 and complementing current norms (gradual innovation). Proposals to introduce a tort for the misuse of personal information by data traders,[40] to provide legal recognition of data harms by extending developments from other areas of the law, such as torts and contracts,[41] to enact a Consumer Privacy Bill of Rights Act,[42] and to expand consumers' rights to access their data records within reasonable timeframes,[43] are all examples of gradual legal innovations that leave core elements of the current regulatory approach unchanged.

[36] J. E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford/New York: Oxford University Press, 2019).

[37] See U. Gasser, 'Perspectives on the Future of Digital Privacy', *Zeitschrift für Schweizerisches Recht* 134 (2015), 338–448, at 368–369. On the innovation-enabling function of law, see also A. Chander, 'How Law Made Silicon Valley', *Emory Law Journal* 63 (2014), 639–694.

[38] Ibid., at 368–369.

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

[40] See S. Ludington, 'Reining in the Data Traders: A Tort for the Misuse of Personal Information', *Maryland Law Review* 66 (2006), 140–193, at 173.

[41] See Solove and Citron, note 31.

[42] See The White House, note 8.

[43] M. Korolov, 'California Consumer Privacy Act (CCPA): What You Need to Know to Be Compliant', *CSO*, 4 October 2019, available at www.csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html.

3. A more radical, paradigm-shifting approach is deeper-layered law reform where not only are individual norms updated, but also entire approaches or instruments are changed. In addition to the proposals already mentioned in the introduction, examples in this category include efforts to reimagine privacy regimes based on models that emerged in the field of environmental law,[44] to reformulate the current crisis as data pollution and develop social instruments that address the external harms associated with the collection and misuse of personal data,[45] to create an alternative dispute resolution scheme, such as a 'cyber court' system to deal with large-scale privacy threats in the digital age,[46] 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,[47] to name just a few illustrations.

Perhaps the most interesting, and arguably the most promising, approach to reprogramming information privacy and data protection law in a more fundamental sense stems from such a paradigm-shifting approach: to embrace the multi-faceted, functional role of law and reframe technology, as 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 under the header of 'Privacy-Enhancing Technologies' (PETs) started to develop technical mechanisms in response to privacy challenges associated with new information and communication technologies.[48] 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 similar instruments have broadened over time to include encryption tools, privacy-preserving analysis techniques, data management tools, and other techniques that cover the entire lifecycle of personal data. Starting in the 1990s, PETs, one instrument in a toolbox of many more, were put into a larger context by the introduction of privacy by design, a 'systematic approach to designing any technology that embeds privacy into [both] the underlying specification or architecture'[49] and, one might add, business practices. Although still a

[44] See D. D. Hirsch, 'Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law', *Georgia Law Review* 41 (2006), 1–63.

[45] O. Ben-Shahar, 'Data Pollution', Coase-Sandor Working Paper in Law and Economics No 854 (2018).

[46] See L. M. Ponte, 'The Michigan Cyber Court: A Bold Experiment in the Development of the First Public Virtual Courthouse', *North Carolina Journal of Law and Technology* 4 (2002), 51–91.

[47] J. M. Balkin and J. Zittrain, 'A Grand Bargain to Make Tech Companies Trustworthy', *The Atlantic*, 3 October 2016.

[48] See G. W. van Blarkom, J. J. Borking, and J. G. E. Olk (eds), *Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents* (The Hague: CBP, 2003).

[49] I. S. Rubinstein, 'Regulating Privacy by Design', *Berkeley Technology Law Journal* 26 (2011), 1409–1456, at 1411–1412.

somewhat amorphous and evolving concept that seeks to integrate legal and technical perspectives, privacy by design can be understood as an important movement that promotes a holistic approach to managing the privacy challenges that result from a wide range of emerging technologies across their life cycles and within their contexts of application. The concept has been endorsed by privacy regulators from across the globe[50] and adopted on both sides of the Atlantic, with the GDPR among the most prominent recent examples.[51] In addition to research efforts and scholarly contributions that deepen, advance, and critically examine the privacy by design concept, a range of implementation guidelines and methodologies have been issued by regulatory authorities, standards organizations, and other sources to help operationalize typically abstract privacy-by-design-requirements.[52] Despite all the progress made, careful examinations of the approach have highlighted both conceptual questions[53] and implementation challenges,[54] including economic obstacles, interoperability barriers, and usability and design issues.[55] Conversely, additional work is also required to close privacy law's 'design gap', at least in practice.[56]

D REIMAGINING THE RELATIONSHIP OF LAW AND TECHNOLOGY

This relatively recent 'discovery' of technology as an approach to address the very privacy challenges it (co-)creates in the law has potential. The more technical dimensions to regulating information privacy have been the focus of intense study by computer scientists and resulted in a rich theoretical literature and numerous practical tools for protecting privacy. Yet, in the past such discussion has by and large occurred in

[50] See 'Resolution on Privacy by Design', *32nd International Conference of Data Protection and Privacy Commissioners*, Jerusalem, 27–29 October, 2010; also C. Perera et al., 'Designing Privacy-Aware Internet of Things Applications', *Information Sciences* 512 (2020), 238–257; M. Veale, R. Binns, and J. Ausloos, 'When Data Protection by Design and Data Subject Rights Clash', *International Data Privacy Law* 8 (2018), 105–123; A. Romanou, 'The Necessity of the Implementation of Privacy by Design in Sectors Where Data Protection Concerns Arise', *Computer Law and Security Review* 34 (2018), 99–110.

[51] Specifically, Article 25 GDPR requires that data controllers, in order to protect the rights of data subjects, implement appropriate technical and organizational measures designed to both embed data protection principles and integrate safeguards into data processing. See, e.g., L. A. Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements', *Oslo Law Review* 4 (2017), 105–120.

[52] See, e.g., G. Danezis et al., *Privacy and Data Protection by Design – From Policy to Engineering* (Heraklion: ENISA, 2014); European Data Protection Board, Guidelines 4/2019 on Article 25: Data Protection by Design and by Default, 13 November 2019.

[53] See, e.g., D. K. Mulligan and K. A. Bamberger, 'Saving Governance-by-Design', *California Law Review* 106 (2018), 697–784.

[54] S. Spiekermann-Hoff, 'The Challenges of Privacy by Design', *Communications of the ACM* 55 (2012), 38–40.

[55] A. Tamò-Larrieux, *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things* (Berlin: Springer, 2018).

[56] See W. Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge, MA: Harvard University Press, 2018).

a space separate from the sphere of legal norms, regulations, policies, ethics codes, and best practices. In addition to the larger shifts mentioned earlier in this chapter, a number of *specific trends* make it now more important as well as urgent to foster knowledge sharing and integration between the two spheres and to embrace technological approaches to support legal privacy across a number of different functions.

First, technological advances enable sophisticated attacks that were unforeseen at the time when many of the still-applicable legal standards for privacy protection were drafted. Computer scientists now need to develop approaches that are robust not only against new modes of attack, but also against unknown future attacks, in order to address challenges posed by next-generation privacy threats.[57] For example, database reconstruction attacks have already demonstrated that large collections of data such as the United States Census – although ostensibly confidential – are now vulnerable to discovery of a particular individual's personal, private characteristics, so new means of protection for these datasets are required.[58] Similarly, the omnipresence of predictive analytics makes it difficult for individuals to understand and control the usage of their own data, rendering traditional regulatory control paradigms increasingly ineffective against developments in technology.[59]

Furthermore, patchworks of privacy laws, the lack of interoperability among them, and different interpretations of their requirements can all result in wide variations in the treatment and protection of data across contexts and geographies, depending on the jurisdictions, industry sectors, actors, and categories of information involved. More robust frameworks for evaluating privacy threats that are based on integrated legal and scientific standards for privacy protection are required to provide more comprehensive, consistent, and robust information privacy protection, thereby furthering the end goals of the law.

Finally, traditional legal approaches for protecting privacy while transferring data, making data-release decisions, or drafting data-sharing agreements, among other activities, are time-intensive and not readily scalable to big data contexts at a time when some of the biggest global challenges urgently require more, not less, privacy-respecting data sharing. Technological approaches need to 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.[60] For example, personalization of the conventional means of ensuring privacy, such as disclosure mandates, could help incorporate more granular legal norms and requirements into an individual's privacy in a scalable fashion.[61]

[57] A. Wood et al., 'Differential Privacy: A Primer for a Non-technical Audience', *Vanderbilt Journal of Entertainment and Technology Law* 21 (2018), 209–276.

[58] S. Garfinkel, J. M. Abowd, and C. Martindale, 'Understanding Database Reconstruction Attacks on Public Data', *ACMQueue* 16 (2018), 1–26, at 5–7.

[59] D. D. Hirsch, 'From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics', Ohio States Public Law Working Paper No 506 (2019).

[60] M. Altman, S. Chong, and A. Wood, 'Formalizing Privacy Laws for License Generation and Data Repository Decision Automation', *Proceedings on Privacy Enhancing Technologies* 2 (2020), 1–19.

[61] C. Busch, 'Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law', *University of Chicago Law Review* 86 (2019), 309–331, at 312.

https://doi.org/10.1017/9781108919234.013 Published online by Cambridge University Press

These reasons already indicate that the need for enhanced *interoperability* between technological and legal approaches to privacy is not limited to the mechanical level of individual privacy-preserving techniques and tools and goes beyond efforts to require companies to protect privacy by embedding it into the design of technologies and business practices. Rather, the scale of the challenge of reimagining the relationship between technology and privacy – as well as the potential benefits of increased levels of interoperability between the two – becomes visible when considering the variety of interrelated functional perspectives that such an approach situated at the law/technology interface would open up when dealing with the privacy challenges of the digital age. The following questions can be raised in this context.

1. How can technological and legal perspectives be integrated more closely to enable more robust problem descriptions and analyses? Approaches like privacy by design signal a departure from binary notations of privacy and ad hoc balancing tests of competing interests toward more holistic and rigorous privacy risk assessment models that rely both on modeling approaches from information security and an understanding of privacy informed by recent theoretical advances across different disciplines. Technical research, for example, may better quantify the privacy risks associated with more traditional privacy-protection techniques like anonymization[62] and thus help establish a legal framework that articulates which privacy risks should be considered 'unacceptable'. Similarly, using both computational and sociological measures could establish a more empirical evidence base about consumers' attitudes and expectations towards privacy.[63] A growing body of interdisciplinary research demonstrates the theoretical and practical promise of such modern privacy analyses that are based in holistic analytical frameworks incorporating recent research from fields ranging from computer science and statistics to law and the social sciences.[64] Indeed, such frameworks are increasingly recognized by expert recommendations and standards.[65]

[62] W. H. Lee et al., 'Quantification of De-anonymization Risks in Social Networks', *ICISSIP 2017 – Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, 1 January 2017.

[63] S. Barth and M. D. T. de Jong, 'The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review', *Telematics and Informatics* 34 (2017), 1038–1058.

[64] For examples from research that illustrate the benefits of such a blended approach, see M. Altman et al., 'Towards a Modern Approach to Privacy-Aware Government Data Releases', *Berkeley Technology Law Journal* 30 (2015), 1967–2072; and I. S. Rubinstein and W. Hartzog, 'Anonymization and Risk', *Washington Law Review* 91 (2016), 703–760.

[65] R. M. Groves and B. A. Harris-Kojetin (eds), *Multiple Data Sources, and Privacy Protection: Next Steps* (Washington, DC: The National Academies Press, 2017); S. L. Garfinkel, 'De-identifying Government Datasets', NIST Special Publication 800-188 (2016).

2. How can legal and technological tools be combined in order to enable more effective, scalable, and accountable solutions to privacy problems, including the need for trustworthy data sharing? A wealth of research and practical examples show how emerging technical privacy solutions, including sophisticated tools for data storage, access control, analysis, and release, can act in concert with legal, organizational, and other safeguards to better manage privacy risks across the different stages of the lifecycle of data.[66] Consider, for instance, the important role encryption plays in securing access to and storage of data,[67] 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,[68] the movement in AI towards transparent and explainable automated decision-making that makes technology more accountable,[69] or the development of technical ways to implement the right to be forgotten by deleting an individual's records from machine learning models efficiently.[70] Formal mathematical guarantees of privacy can also reliably lower privacy risks. Differential privacy is one such example of a mathematical framework that manages the privacy challenges associated with the statistical analysis of information maintained in databases.[71] Secure multiparty computation, to add another example, is a methodology 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.[72] 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. Real world examples include the implementation of differential privacy in the United States Census,[73] as well as the use of security multiparty

[66] See, e.g., 'Privacy Tools for Sharing Research Data', Harvard University Privacy Tools Project, available at https://privacytools.seas.harvard.edu/project-description.

[67] For a description of encryption standards for federal government information systems, see, for example, National Institute of Standards and Technology, Security Requirements for Cryptographic Modules: Federal Information Processing Standards, Federal Information Processing Standards Publication, FIPS PUB 140-2, 25 May 2001.

[68] See T. Kirkham et al., 'The Personal Data Store Approach to Personal Data Security', *IEEE Security and Privacy* 11 (2013), 12–19, at 12–13.

[69] S. Wachter, B. Mittelstadt, and L. Floridi, 'Transparent, Explainable, and Accountable AI for Robotics', *Science Robotics* 2 (2017).

[70] M. Hutson, 'Researchers Can Make AI Forget You', *IEEE Spectrum*, 15 January 2020.

[71] *See* C. Dwork, 'Differential Privacy', in H. C. A. van Tilborg and S. Jajodia (eds), *Encyclopedia of Cryptography and Security*, 2nd edn (New York: Springer, 2011), 338–340.

[72] See Y. Lindell and B. Pinkas, 'Secure Multiparty Computation for Privacy-Preserving Data Mining', *Journal of Privacy and Confidentiality* 1 (2009), 59–98, at 60.

[73] United States Census Bureau, 'Disclosure Avoidance and the 2020 Census', 19 December 2019, available at www.census.gov/about/policies/privacy/statistical_safeguards/disclosure-avoidance-2020-census.html.

https://doi.org/10.1017/9781108919234.013 Published online by Cambridge University Press

computation to investigate pay gaps,[74] or maintain data on student outcomes in higher education.[75]

3. How can enhanced levels of interoperability between technological and legal approaches to privacy enable better matching of solutions to problems? The Harvard University Privacy Tools Project, for example, is a multidisciplinary effort to develop technical tools to address specific, identified policy needs.[76] Among other contributions, the project demonstrates, for certain categories of use cases, including data sharing in research contexts, how interdisciplinary approaches can guide actors to engage in more robust privacy risk assessments and then select the best solution from a set of integrated privacy tools, such as tiered access models, that combine both legal and technical approaches to privacy protection.[77] As another example, the LINDDUN approach, developed at Leuven University, creates a taxonomy of mitigation strategies to address privacy threats in a given high-level system and identifies effective, targeted PETs by creating data flow diagrams, mapping privacy threats, and performing risk analyses on these privacy threats.[78]
4. How can a closer integration of technical and legal concepts and applications aimed at protecting privacy make it easier to demonstrate compliance and 'measure progress' over time? Again, differential privacy is a key example of using a highly technical conception of 'privacy' to give the vague legal words used to define privacy in statutes and regulations more precision, which in turn increases the accuracy of assessment of compliance in individual cases and over time.[79] More generally, legal standards could adopt more technically robust descriptions of an intended privacy goal rather than simply endorsing traditional approaches like de-identification. This would provide a clearer basis for demonstrating whether new classes of emerging privacy technologies are sufficient to fulfil the requirements of these standards. These examples indicate how policymakers and technologists could seek to employ a hybrid of legal and technical reasoning to demonstrate a privacy solution's compliance with legal standards for privacy protection.[80]

[74] R. Barlow, 'Computational Thinking Breaks a Logjam', Boston University, 27 April 2015, available at www.bu.edu/articles/2015/computational-thinking-breaks-a-logjam.

[75] M. R. Warner, 'Warner, Rubio, Wyden Reintroduce "Student Right to Know before You Go Act"', *Press Release*, 7 March 2019, available at www.warner.senate.gov/public/index.cfm/2019/3/warner-rubio-wyden-reintroduce-student-right-to-know-before-you-go-act.

[76] Harvard University Privacy Tools Project, note 66.

[77] See, e.g., Altman et al., note 64.

[78] 'LINDDUN Privacy Engineering', *LINDDUN: Privacy Threat Modeling*, available at www.linddun.org/.

[79] K. Nissim et al., 'Bridging the Gap between Computer Science and Legal Approaches to Privacy', *Harvard Journal of Law and Technology* 31 (2018), 687–780.

[80] Ibid.; Nissim and Wood, note 32; A. Cohen and K. Nissim, 'Towards Formalizing the GDPR's Notion of Singling Out', *arXiv*:1904.06009, 12 April 2019, available at https://arxiv.org/abs/1904.06009.

https://doi.org/10.1017/9781108919234.013 Published online by Cambridge University Press

Taken together, the integration of legal and technical approaches across different functional areas can 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 and data protection. The process of reimagination through enhanced interoperability – here illustrated along four functional areas with the open-ended possibility of adding others – builds heavily upon the concept of privacy by design and is informed by related approaches such as privacy impact assessments. However, as already mentioned, this process is less focused on embedding privacy requirements into the design and architecture of individual technological systems and business practices. Rather, it is more broadly interested in finding ways to overcome the traditional interaction patterns between technology and law in order to offer new system-level opportunities to develop notions and manifestations of privacy that might only emerge after combining different substantive and methodological 'lenses'. At a moment of rethinking privacy, such an exercise might inform the evolutionary path of privacy and data protection laws at both the conceptual and implementation levels by challenging their underlying assumptions, definitions, protection requirements, compliance mechanisms, and so on.

E TOWARDS RECORDING PRIVACY LAW

Over time, enhanced interoperability between technological and legal approaches to privacy might ultimately culminate in a deeper-layered *recoding* of privacy law that transcends the traditional response patterns[81] discussed earlier in this chapter by leveraging the synergies between perspectives and instruments from both domains in order to cope with the complex privacy-relevant challenges of our future. The path towards such an outcome, however, is long and faces many obstacles given the economic, geopolitical, and other forces at play that were described earlier in this chapter.

As a precondition of any progress, such a strategy requires significant investments in interdisciplinary education, research, and collaboration.[82] Despite all the advancements made in recent years, 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 roles for law and legal governance in such a dynamic, fast-changing system. Programs designed to stimulate such collaboration and interdisciplinary learning have already started being

[81] See also H. Burkert, 'Changing Patterns: Supplementary Approaches to Improving Data Protection', *Presentation at CIAJ 2005 Annual Conference on Technology, Privacy and Justice*, Toronto, 2005.

[82] See, e.g., US National Science and Technology Council, 'National Privacy Research Strategy', White House, June 2016, available at https://obamawhitehouse.archives.gov/sites/default/files/nprs_nstc_review_final.pdf.

developed at universities.[83] Furthermore, technology positions in government, such as the Chief Technologist position at the Federal Trade Commission and the President's Council of Advisors on Science and Technology, to name two examples from the United States, recognize the need for experts in computer science who can inform privacy regulation and serve as models of cross-disciplinary communication and knowledge-sharing in policy circles.[84] 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 such standards. Doing so will also likely require policymakers to develop mechanisms and resources for communicating their shared understanding of the interface between law and technology with privacy practitioners. Regulatory systems and institutions will also need to support additional research on policy reasoning, accountable systems, and computable policies for automating compliance with legal requirements and enforcement of privacy policies.[85]

Reimagining the relationship between technology and privacy law in the digital age can be seen as a key component of a larger effort aimed at addressing the current digital privacy crisis 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 professional practices, and the law. If pursued diligently and collaboratively, and

[83] Examples in the field of research are initiatives such as the Privacy Tools for Sharing Research Data at Harvard University mentioned earlier, which brings together computer scientists, statisticians, legal scholars, and social scientists to tackle difficult problems at the intersection of privacy technology, or the efforts by the Center on Privacy and Technology at Georgetown University Law Center, which aims to build interdisciplinary bridges between law and computer science 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., Massachusetts Institute of Technology, Course: Privacy Legislation: Law and Technology, available at https://groups.csail.mit.edu/mac/classes/6.S978; Harvard Law School, Course: Comparative Online Privacy, available at http://hls.harvard.edu/academics/curriculum/catalog/default.aspx?o=69463; Carnegie Mellon University, Course: Privacy Policy, Law, and Technology, available at https://cups.cs.cmu.edu/courses/pplt-fa16; A. Narayanan, Privacy Technologies: An Annotated Syllabus, Princeton University, available at www.cs.princeton.edu/~arvindn/publications/privacyseminar.pdf.

[84] See L. Sweeney, 'Technology Science', *Federal Trade Commission Blog*, 2 May 2014, available at www.ftc.gov/news-events/blogs/techftc/2014/05/technology-science.

[85] See, e.g., D. J. Weitzner et al., *Computer Science and Artificial Intelligence Laboratory Technical Report: Information Accountability* (Cambridge, MA: MIT Press, 2007); L. Kagal and J. Pato, 'Preserving Privacy Based on Semantic Policy Tools', *IEEE Security and Privacy* 8 (2010), 25–30; H. 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* (New York: ACM, 2010), 73–82; US National Academies of Sciences, Engineering, and Medicine, *Innovations in Federal Statistics: Combining Data Sources While Protecting Privacy* (Washington, DC: The National Academies Press, 2017); Groves and Harris-Kojetin, note 65.

expanding upon concepts, such as privacy by design or privacy impact assessments, as written into modern privacy frameworks like the GDPR, such a turn toward *coordinated privacy governance* could result in a future-oriented privacy framework that spans a broad set of norms, control mechanisms, and actors[86] – 'a *system* of information privacy protection that is much larger, more complex and varied, and likely more effective, than individual information privacy rights'.[87] Through such nuanced intervention, the legal system (understood as more than merely a body of constraining laws) can more proactively play the leading role in directing and coordinating the various elements and actors in the blended governance regime, and – above all – in ensuring the transparency, accountability, and legitimacy that allow democratic governance to flourish.[88]

[86] See C. J. Bennett and C. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, MA: MIT Press, 2006).

[87] V. Mayer-Schönberger, 'Beyond Privacy, Beyond Rights – Toward a "Systems" Theory of Information Governance', *California Law Review* 98 (2010), 1853–1885, at 1883 (emphasis in the original).

[88] See M. Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Cheltenham: Edward Elgar, 2015).