3

A Mirror, Not a Glass Door

Legal Code and Software Code in Practice

Justin Petelka, Megan Finn, Janaki Srinivasan, Elisa Oreglia, and A. P. Janani

What was supposed to be like a glass door that lets me see through what Google is doing with my data, instead of making this a glass door, they've just made it a mirror.
—Participant P15, India, talking about their Google data

In this chapter, we explore the uneven and shifting practices of data access rights through the experiences of people requesting their data from different companies in India, the United Kingdom, and the United States in 2019–21. This is the period after the General Data Protection Regulation (GDPR) of the European Union (EU) went into effect in 2018 and during a period of legal change, in the United States with the implementation of the California Consumer Privacy Act (CCPA) in June 2020, and in India with the drafting of the 2019 Digital Personal Data Protection Bill.[1] While the GDPR applies to data processed within the EU or from EU residents, we argue that GDPR's scope in this period extended beyond EU borders because multinational company infrastructures extended from the EU to countries with different regulations, compliance and enforcement protocols, and even cultural conceptions of data privacy. Building on analyses of *written laws,* we evaluate the influence of the GDPR beyond the EU (called the Brussels Effect) and the CCPA's influence within the United States (called the California Effect) by analyzing *data infrastructure* outputs.[2] We explored the byproducts of both legal code and software code by working with research participants in the three countries to request, and to examine the process of requesting and accessing, their personal data from the same multinational companies and regionally operating companies. Our research articulates what we call *trickle-down GDPR*, an important mapping of the ways corporations translate national laws into their technical infrastructure and then how people ultimately experience those laws in different regions.

Rather than focusing only on legal doctrine or technical infrastructure, we map individuals' experiences of both in a concrete, ground-up way in order to understand the connection between the making and the intended effect of laws, and the actual practices that emerge from these

laws and technical infrastructures. We interviewed 19 participants in the United States, India, and the EU who made 38 unique data subject access requests (DSARs) to companies, and we documented their experience of this process. We show that trickledown GDPR does appear to be real: companies that fulfilled data access requests in the EU also extended those rights to data subjects in India and the United States. Companies that do not operate in the EU, however, mostly did not respond to data requests. There were exceptions: one US company that did not operate in the EU inconsistently responded to data requests, and participants in India were unable to access data from Amazon. We examine the wide variability in companies' interpretation of GDPR legal code as incorporated in the software code which powers the infrastructures that process data.

The experience of people requesting access to their personal data is not reducible to just the legal code or the software code: any analysis of the efficacy of the GDPR and similar laws must consider the lived experiences of users too. While we show that data access rights exist for non-EU citizens and residents who are requesting data from companies that operate in the EU, we are also circumspect about how these rights are meaningful. Further, these experiences of users also introduce new questions such as, How do GDPR's data access rights address information asymmetries between civilians and tech corporations? Data requests are expected to provide a certain level of transparency and be a cornerstone of data protection, but most of our research participants felt that GDPR and data access rights did not allow them to catch a glimpse of the companies' inner workings as they expected—they were a mirror, not a glass door.

In the chapter epigraph, we invoke *An Engine, Not a Camera*, in which author Donald MacKenzie showed that financial economics was in fact "an active force transforming its environment, not a camera passively recording it."[3] Whereas many participants were expecting a glass door they could peer through to see some of the logic and modus operandi of a data controller, they instead found a mirror—a reflection of only *themselves* in their data. Furthermore, when people requested access to personal data, what data companies had about people remained unclear. Despite the performance of transparency (and compliance with transparency-focused laws like GDPR), no participant could read corporate privacy policies or see their data and come away with an idea of which data were being collected by the company, how they were kept, or what purpose the data serve for the company. The companies produced the problem of personal data access and, through control of the corporate infrastructure, the supposed solution: the process of data request and access.

This paper unfolds over two parts. The first describes the scholarly background that helped us map the relations between legal code and software code. The second part describes our efforts to understand how software code and legal code translate into user experiences. In the first part,

we begin with personal data access in different legal regimes in the EU, United States, and India. We then discuss different conceptualizations of the application of local laws to transnational infrastructures. Following this review of legal regimes and their deployment in transnational contexts, we discuss the scholarship on GDPR compliance practices. In the second part, we describe our research process, starting with our research design, structured to understand whether and how different companies (both those that operate across and those that operate within regions of our study) incorporate the GDPR into the process of personal data requests.

Legal Code and Software Code

The next two subsections describe the different historical and political backgrounds of the EU's, United States', and India's approaches to data protection and data regulation. Rights of access, rectification, cancellation, and objection (ARCO) are now defined and protected by different laws and regulations in different jurisdictions, particularly the European Union's 2018 GDPR. The 1995 Data Protection Directive (DPD95) and the GDPR created requirements for organizations that collect and process "personal data," called "data controllers."[4] Among the requirements for data controllers is to recognize a series of informational rights granted to "data subjects." To comply with these obligations, EU organizations in every sector implemented procedures for rights bearers to access their personal data—reflecting a concept with a history reaching back a half century.[5]

European legislators began discussing the idea of data protection, including the right of access to personal data, more than 50 years ago. Increasing international data flows and widespread access to telephony, data storage, and databases created issues of jurisdiction; in response, some European regions passed data protection laws in the 1970s.[6] This legislation signaled the beginning of tensions around data flows that are still playing out today between multinational corporations and states. Corporations argued that information was immaterial—a special kind of good that cannot be depleted and needs other information to multiply. European states, however, saw information as another good, produced in specific places, whose flow and boundaries had to be controlled by the state itself or through international agreements. These two perspectives together provided scaffolding for the growing production of information as a commodity. The Organisation for Economic Co-operation and Development (OECD), the European Economic Community (EEC), and other entities, began to issue data protection laws and attempted to regulate international data flows.[7] Alongside these efforts, "developing countries" started to push back against the free flow of information, which they saw as asymmetrical.[8] In the late 1980s and early 1990s, the emergence of the World Wide Web, with its supranational standards and governance, the

increasingly global presence of US tech companies, and the libertarian politics that underpinned the computing industry of this era slowed attempts at global regulation of transnational data flows.[9] Yet European countries continued to enact national data protection laws, which were harmonized into a single cohesive framework by the EU through the DPD95, followed by the GDPR.[10]

The right of data subjects to request the data held about them through a DSAR is a cornerstone of GDPR and the subject of this chapter.[11] Legal scholars Jones and Kaminski argue that ARCO rights such as DSARs are crucial to data protection: "Only through knowing about and participating in what information governments and companies hold on them can individuals check unchecked power, regain some (but not absolute!) control, and push back against manipulation in the information age."[12] Thus, DSARs can be understood as a form of information transparency like that emerging from the Freedom of Information Acts (FOIAs) in the United States and United Kingdom and the Right to Information Act (RTI) in India.[13] While individual data access is one of the fundamental building blocks in the GDPR's complex regulatory scheme, DSARs cannot alone ensure data protection, as Ausloos and Dewitte have argued: "The right of access both acts as a necessary first step enabling the exercise of most other data subject rights, and *as a strategic tool to assess compliance with data protection law more broadly*."[14] Thus, though data access has limited effectiveness in regulation and is focused on individual rights, "the right of access can therefore be a vehicle not just at an individual level but also as the catalyst to pursue legislative reform and policy considerations."[15] The potential of DSARs to check power asymmetries lies in collective action.[16]

Alternative Approaches to Data Regulation

By comparison, US approaches to ensuring privacy and protecting data from corporations are not based on natural rights or collective harms. The implicit assumption parroted by corporations is that consumers trade personal data for goods and services by consenting to different legal agreements. However, this transactional approach obscures the fact that users don't know what data are collected about them and that platforms share their data with other, undisclosed organizations. The current transactional approach to consumer data was not always the case, as illustrated by the National Data Center efforts in the 1960s, the Fair Credit Reporting Act of 1970, the Ware reports, the Department of Health, Education and Welfare 1973 report (which included a first description of Fair Information Practices [FIPs]), and the US Privacy Act of 1974.[17]

Today, US information privacy rights are enacted through a patchwork of sector-specific laws, often through regimes of notice-and-choice in which individuals are treated as consumers who theoretically can decide

whether to participate in using a service based on transparent and accurate descriptions of data collection by different entities.[18] This individualized consumer model presumes rational deliberation and real choice—an approach to privacy that does not reflect how people actually work.[19] While the consumer model's appeal in the United States has deep ties to notions of progress, technology, and innovation, the gap it creates between the imagined citizen of US market discourse and a real citizen is a legal fiction according to which consumers are presumed to have read and understood a company's data practices when they accept the terms of a privacy notice.[20]

The US approach to privacy has resulted in data protection laws distinct from the EU tradition, such as the California Consumer Privacy Act (CCPA), which became effective January 1, 2020.[21] The CCPA and other state data laws such as Virginia's Consumer Data Protection Act oblige for-profit entities that collect consumer personal data to recognize the rights of state residents, such as the right to access personal data and other ARCO rights.[22]

The informational rights regime in India appears to draw on both the European and American values described above and aspects of the local legal landscape and politics. India's Digital Personal Data Protection Act was passed in 2023, though a data protection law had been discussed since at least 2017. The 2023 law came from a fresh draft of a bill that was tabled in 2022, after the 2019 version was scrapped. Many aspects of the 2023 law, as well as the preceding 2019 draft bill and the Srikrishna Committee report of 2018, appear to mirror the GDPR. These legal documents share the broad definition of "processing" of data, many forms of data are classified as "sensitive," and they include the requirements of data minimization, purpose limitation, and consent.[23]

While influenced by the GDPR, India's Data Protection Act and draft bills were also influenced by the reaffirmation of privacy as a fundamental constitutional right based on the 2017 Puttaswamy judgment of the Indian Supreme Court.[24] The Srikrishna Committee highlighted in its expert report that the "core of informational privacy is a right to autonomy and self-determination in respect of one's personal data. Undoubtedly, this must be the primary value that any data protection framework serves."[25] The Indian act (and earlier draft bills) differ significantly from the GDPR in the exceptions it makes for the state; legal scholar Graham Greenleaf has labeled a previous draft "GDPR-lite with Chinese characteristics."[26] Another important provision in the 2023 act is its amendment to the Right to Information Act that abolishes the obligation to provide a citizen any information seen as personal (thus providing an absolute rather than a conditional exemption).[27] As of this writing, the provisions of the Indian Personal Data Protection Act and the draft rules required to operationalize the act that were released for public consultation in January 2025 are

subjects of fierce debate in academic, popular, and policy circles,[28] particularly against the backdrop of the country's recent pervasive use of digital ID systems,[29] the 2018 National Policy on AI, the national Automated Facial Recognition System, and, ironically, the act's amendments to the Right to Information Act that would reduce the ability of citizens to access information.[30]

Translating Legal Code into Technical Code

We recruited participants from three countries—the United States, the United Kingdom, and India—with different legal regimes in order to understand the interaction of transnational and local laws in 2019–21. The potentially internationalizing qualities of the web set up tensions between local laws and global infrastructures. On one hand, examining the laws of different regions often showcases variations in interpretation of words by class, work expertise, and geography. In *Trying Leviathan*, Burnett shows how a trial about whale oil regulation ultimately hinged on whose categorization of a whale would prevail—the naturalist's as a mammal or the layperson's as a fish. In the New York case of *Maurice v. Judd* (the subject of *Trying Leviathan*), the interpretation of locals held primacy over the interpretation of nonlocal "easterners."[31] On the other hand, a transnational organization must negotiate multiple, sometimes conflicting, national laws in order to maintain business activities in different countries, including development and deployment of technical infrastructure. IBM, one corporation with a global footprint, set a historical precedent by working within and shaping many legal and political regimes.[32]

Given the ambitions of personal data access and the nature of transnational corporations that must comply with the GDPR within EU borders, a closer look at how EU laws shape global practices is warranted. Legal scholar Anu Bradford has characterized the transatlantic impact of EU regulation as the "Brussels Effect," suggesting that the EU can unilaterally regulate global markets through market mechanisms.[33] Paul M. Schwartz suggests, however, that the expansion of EU law has more to do with the appeal of high standards for data protection and its portability to other legal contexts.[34] The diffusion of legal regimes for data protection into low-resource countries may also play into historical arcs of marginalization and colonization.[35] Studies of on-the-ground privacy practices and belief show variability in expectations and understanding of "privacy" across countries and within them, based on social position.[36] For instance, ideas about privacy vary within India based on people's social position and their varied encounters with the state.[37]

Our study suggests that in addition to EU influence on laws, the power of the GDPR lies in transforming other nations' digital infrastructures. As Jones and Kaminski argue, this transformative effect is deliberate: "Much of the work the GDPR aspires to do is beneath the surface, changing cor-

porate infrastructure and processes and reprioritizing decision-making around data protection rights and values."[38] Thus, the impact of the GDPR regulation emerges materially in private internet infrastructures that extend beyond EU borders. GDPR requires that states and corporations work together to enact the regulation in an arrangement called "collaborative governance."[39] The ongoing collaborative governance between transnational corporations that operate infrastructure and the EU creates border-crossing material infrastructure that sits in the gap between "law in books" and "law in action."[40] The results of data requests are the material representations of the law in action or the ways a corporation has enacted GDPR.[41]

Understanding the Impact of the GDPR

Theoretical and legal scholarship on rights in the EU analyze the legal and historical contexts of international data policy and interpret the requirements of law.[42] In contrast to law in books, scholarship on ARCO rights in practice (law in action), breaks apart the exercise of data rights into smaller subprocesses and focuses on evaluating company compliance. While it is possible to see how written laws compare with one another, it is much harder to see how different companies have interpreted and enacted the GDPR and how they have translated the legal code into software code that enables something like a DSAR. While there are provisions in the GDPR for auditing, the audits are not required to be public.[43] Scholars have thus adopted a range of approaches to analyzing GDPR's effects through automated measurements of GDPR compliance such as privacy policy statement length, topics covered in privacy policies, requirements of data portability requests, and security risks to data subjects and data controllers.[44]

In the US context, law and technology scholar Ari Waldman argues that rendering data privacy laws ineffective is not an accident but a product of one of the core goals of data privacy law, which, both in the United States and globally, is to make privacy "doable" for companies.[45] Waldman borrows the concept of *legal endogeneity* from socio-legal scholar Lauren Edelman to describe how data privacy law does not constrain, restrict, or guide regulated entities but is instead shaped by the regulated entities themselves.[46] Data privacy laws provide compliance professionals (e.g., lawyers, engineers, privacy professionals, and risk managers) a wide berth to interpret what "compliance" means in practice and to design processes by which to fulfill corporate goals of efficiency and profitability that act as symbols of following the law. These symbolic structures in turn shape the everyday practices of judges, regulators, data controllers, and data subjects who, over time, normalize these symbols as adequate data protection and privacy measures and even hail them as groundbreaking. Similarly Con Diaz's history of patent law explains how corporations' interpretation of the concept of software, and thus what is regulated, are

bound to their interests.[47] In the area of DSARs, corporations have substantive leeway in interpreting the GDPR; this research suggests that corporations decide how to implement GDPR within their technical infrastructures so as to obey the letter but not the intention of the law.

Researchers have also assessed the "practical reality" of exercising ARCO rights in the EU by using various rubrics, such as success versus failure, compliant versus noncompliant, complete versus incomplete, easy versus difficult, and satisfactory versus unsatisfactory.[48] These approaches to analyzing the technical infrastructure of both automated methods and DSAR compliance metrics is important for ensuring GDPR compliance. However, they do not necessarily capture the gaps in human experience of engaging with such infrastructure, mediated by users' own technical infrastructure, skills, and expectations, or the meaning making that happens as people make sense of their experiences dealing with a corporation's technical infrastructures. Our DSAR-focused study seeks to add an additional layer of analysis to Norris and colleagues "law in action" by looking not only at results but also at processes in order to understand some of the practical accomplishments of GDPR in the EU and beyond.

Personal Data Requests and Data Access in Practice

To understand how DSARs are addressed in different legal regimes, we recruited 19 participants from India (7 participants), the United States (6), and the United Kingdom (6). Data collection was conducted in overlapping phases through surveys and interviews between September 2019 and March 2021. Crucially, all UK access requests were completed (and data retrieved) before the United Kingdom left the European Union on January 31, 2021, and all US requests were completed after the CCPA came into effect on January 1, 2020, by participants outside California and prior to the passage of India's 2023 Personal Data Protection Act. Participants were recruited from single states (Washington in the United States, Karnataka in India) or nations (England in the United Kingdom) through our personal networks. Our participants were residents of these states but were not necessarily citizens and tended to have high levels of education.

In addition to understanding how DSARs are experienced with transnational companies in different countries, we also wanted to find out how DSARs worked in companies that did not operate across all three regions, and whether *transnational* and *domestic* companies had different practices. Understanding whether transnational companies fulfilled DSAR requests outside the EU and whether companies that did not operate in the EU fulfilled DSAR requests helped us understand the reach of the GDPR. We selected several transnational companies that operate in all three regions—Google, Amazon, Facebook, and Spotify—and a number of domestic companies that operate in only one of the regions: Monzo and

Ryanair in the United Kingdom; Alaska Airlines and Venmo in the United States; and Reliance Jio, Paytm, and Flipkart in India.[49] In addition to region, we also selected companies based on economic sector, focusing on transnational media, technology, retail sales, and regionally operating aviation and financial companies.

Although we intended to conduct the same protocol in all three regions simultaneously, we ended up using two different protocols. Our initial protocol was inspired by Ausloos and Dewitte's 2018 study.[50] We created a series of questionnaires that walk respondents through the process of requesting personal data from two services and reporting their experiences; after the questionnaires were completed, we interviewed participants. We began recruiting participants in all three regions in September of 2019. While 7 of 10 participants in India completed the initial protocol, participants in the United States and United Kingdom struggled.

We then revised our protocol for US and UK participants, replacing questionnaires with two remote interviews via Zoom to first record people's experiences in making DSARs and then analyzing the data they received. We recruited participants from outside California in the United States (the only state with data privacy laws at the time of the study) and United Kingdom and asked them to send DSARs to two different services. During one- to two-hour interviews, participants were encouraged to think aloud while sharing their screen (only if the participant was reasonably confident a file did not contain any sensitive information).[51] The interviewer also encouraged participants to ask questions if they ran into obstacles—which they consistently did.

Table 3.1 summarizes what our participants received. Our work shows evidence of trickledown GDPR: 27 out of the 38 access requests made by our participants resulted in a participant receiving some kind of data. With the exception of Amazon DSARs from India, all of the transnational companies responded to DSARs with data regardless of the requestor's location. And most, though not all, US and Indian companies that did not operate in the EU did not fulfil data requests. We hypothesize that Venmo, the US company that does not operate in the EU yet complied with DSARs (albeit inconsistently, returning different file formats to different participants), might have been influenced by CCPA. But, since the timing of our work overlapped with CCPA implementation, more research is needed to understand the effects of CCPA and other data protection laws in the United States.[52]

The Experience of Codes

In this section, we discuss our findings, focusing on how access requests worked in different jurisdictions and for different companies. Our description focuses on the process and the results of DSARs because both played an important role in how participants interpreted their rights under data

Table 3.1. Company responses to DSAR requests

Service	Region	Channels used for DSAR	DSAR channel locations	Total data requests	Successful data requests	Total requests analyzed*	Time to complete	Returned data format	User chooses format?	Formats available	*Read me* file included in data returned?
Google	Multiple	Dedicated service	Account settings, help documentation, community help	6	6	6	Same day	Multiple	Yes	Products, delivery method, frequency, file type and size	No
Amazon	Multiple	Dedicated button	Help documentation	6	4	4	5–15 days	Multiple	Yes	Data categories	Sometimes
Facebook	Multiple	Dedicated button	Account settings, help documentation, contact form	7	7	6	Same day	Multiple	Yes	Categories, date range, format, media quality	No
Spotify	Multiple	Dedicated button, chat	Privacy settings, help documentation	5	5	5	2–8 days	JSON	No	N/a	yes
Flipkart	India	Phone, email	Privacy policy	3	0	0	N/a	N/a	N/a	N/a	N/a
Reliance Jio	India	Phone, email	Customer service	1	0	0	N/a	N/a**	N/a	N/a	N/a
Paytm	India	Phone, email, chat	Customer service	2	0	0	N/a	N/a	N/a	N/a	N/a
Venmo	US	Contact form, email, chat	Privacy policy, customer service	2	2	2	20–23 days	PDF, CSV	Sometimes	Data range for CSV	Sometimes
Alaska Air	US	OneTrust request form	Privacy policy	2	0	0	N/a	N/a	N/a	N/a	N/a
Monzo	UK	Contact form, email, chat	Privacy policy, customer service	2	1	1	18 days	PDF	No	N/a	Yes
Ryanair	UK	OneTrust request form	Privacy policy	2	2	1	2–3 days	DOC, web portal	No	N/a	No
Total				38	27	25					

*Number of requests for analysis. (Two participants who received data, P7/Ryanair and P11/Facebook, were unable to go over them at the time of our interview.)
**A RelianceJio representative confirmed which categories of data were being held but emphasized that they could not disclose them to our participants.

protection laws. A complex data request process, followed by files that were not easy to interpret or even to open, influenced people's perception of how transparent the process really was. While past work has framed DSAR activities as successes or failures, the experiences of our participants defied clear metrics. Therefore, rather than framing our findings on the data access request in terms of success or failure, we describe them according to the ways requestors experienced DSARs in order to illustrate the range of ways legal codes were translated into software codes. Both the data that requestors did and did not receive, and the process of making the data request were essential to users' understandings of whether DSARs were actually helping users gain insight into what kinds of personal data corporations held.

Transnational companies (e.g., Facebook, Google, Spotify, and Amazon) have processes for providing data on request. Unlike the processes that domestic companies follow, those of the transnational companies are both integrated (that is, not operated by a third-party service) and at least partially automated. Facebook and Spotify provide "download my data" buttons in their settings, while Amazon places its in the help documentation. Google provides a special service (Google Takeout) for requesting data from all its products separately or at once. Transnational companies usually returned data the same day but took no longer than a week (table 3.1). For those domestic companies that provided data at all, the data was returned within 20 to 23 days (with the exception of Ryanair, who returned data in 2 days).

To the extent that the DSAR and GDPR's informational regime hinges on access, individuals need to be able to request data. Participants often could not figure out how to conduct a DSAR, as we explain with examples from Amazon and Monzo. Of the transnational companies, Amazon posed notable challenges for our participants. In all three countries, participants struggled to identify where and how to download data from Amazon. Ultimately, both participants from India were unable to retrieve any data from Amazon, despite contacting customer service. Where a "download my data" button did not exist, participants faced other challenges. Participant P7 spent several hours trying to request and unlock data from the UK-based payment service Monzo by exchanging emails with the company asking for data and finally scheduling a call with a representative to obtain the password over the phone.

While policy readability serves a critical role in compliance, the approach adopted by our participants highlights that using privacy policies does not reflect the processes users undertake in trying to obtain data.[53] Participants looked at privacy policies less than a third of the time when they were making requests of transnational companies. On the other hand, during almost half of the request attempts, participants used Google with searches such as "access personal data amazon" (P9, UK). Thus, although

data download processes can be touted as streamlined and straightforward, they were not. Comments from our participants warrant future research about how personal data is transferred and combined with data from other firms.

If making a data request took these many forms, the steps involved in receiving the data were no less varied or complex. Since various actors and services are responsible for enabling access requests, the receipt of data could fail in many ways and at several stages. For instance, while requesting data from the UK-based airline Ryanair, P7 encountered OneTrust, a privacy management service. Two days after successfully requesting data, OneTrust sent an expiring link via email to P7, which the participant then used to successfully access their data on OneTrust's web platform. However, P7 was not aware that the link would expire and did not download the data before our interview. Similar to other participants who encountered this problem, we simply rescheduled the interview and P7 remade the request. When we reconvened, P7 noted that OneTrust had not yet sent the expiring link as expected. After some cooperative troubleshooting, we discovered that, coincidentally, Gmail was experiencing an outage and the participant was unable to receive emails at all. We made one more attempt the following day, but ultimately were unable to receive the verification email from OneTrust. This example underlines the complexities of underlying infrastructures that support data access in practice, and also shows that in some cases third parties have at least limited access to personal data.

The Black Box of Data Collection Remains a Black Box for Users

When participants received data, most across geographies described being concerned about what the companies really understood about them, how and why companies had classified them as certain types of users, or why they were given certain kinds of data. Our research participants were not privy to the reasons why companies chose to keep certain data about users and not others. But they were less concerned about this information asymmetry than about the imbalance of power between themselves and corporations.

Participants did not know what to make of the data that were provided to them. They speculated as to whether the data were complete and why certain information was included or excluded—deliberately or because of incompetence. This led to more guessing about the for-profit companies that held the data. Rather than increasing the sense of control, for some participants the process of requesting their data did the opposite. For example, users did not understand why they received data from services they did not use but that were owned by the companies from which they had requested data. A participant making Amazon requests was surprised

to learn that there was data about them associated with an Amazon product (Alexa device) that the participant did not own. When asked whether they thought the data they received were all that the company held on them, one participant expressed confusion: "I obviously do not think that this is all they have. . . . I have no reason to think that they do [have more data] but, yeah, some part of me thinks that they for sure have more stuff. But, yeah, there's no basis for this. It's a gut feeling" (P5, United States, regarding Spotify and Amazon data requests). The participant couldn't know whether these were all the data that a corporation had about them.

The many formats of data added to the confusion and sense of being powerless experienced by participants: they felt upset at being analyzed by companies in ways that were not accessible to themselves. The fact that data came packaged inconsistently as PDF reports, JSON files, or CSV spreadsheets led to frustration. One participant expected "something more in text format, or something even in spreadsheet format. Something, a report, of how am I behaving or how am I interacting with such softwares or application. I wasn't expecting codes and riddles or anything. I have no idea what this is" (P8, UK).

Participants wondered about the link between their behavior on a specific platform. P5, based in the United States, wondered about being labeled an "alcohol buyer" on the basis of Spotify activity despite self-identifying as a practicing Muslim. The corporation's code gave participants access to their personal data, but this only led confused participants to speculate as to whether the data were accurate. Moreover, esoteric formats and categories made participants feel powerless: "It gives me the raw data, but it doesn't really give me any idea necessarily on the power of this data. And especially, and here's another thing, is like my data individually may not be worth a whole lot, but when it is in aggregate with every other customer's data, that's worth a lot. They could do anything they wanted with this information" (P4, United States, Amazon and Alaska Airlines data request). Ultimately, participants expressed a sense of disappointment on realizing that having control of their own data did not mean much in terms of seeing what happens to the data *within* companies.

Expectations about what the GDPR allowed was confusing and sometimes empowering for users both inside and outside the EU. Participants in the EU contrasted their impression that GDPR should enhance transparency with the opaqueness of the process in practice. As P10 (United Kingdom) pointed out, "The interesting thing is that GDPR makes it look like, 'Oh, here, I've got all this control,' but if you actually look at the control it's offering you, it doesn't actually explain that, okay, if I say this, what does it really mean for my browsing future?" (P10, concerning GDPR cookie notices).

Interviewees in India and the United States thought that the GDPR guarantees EU citizens a right to privacy—a popular yet incorrect under-

standing of data protection.[54] Comparison with European experiences came up in several interviews with non-EU participants. For example, P4 (United States) said regarding Amazon data: "I have no way of knowing like if I lived in another country, like if I lived in Europe, would they be obligated to send me more. I have no way of knowing for sure if there is more information on me. I just kind of have to trust that this is all . . . [t]his is all there is." Another participant imagined that, for companies that carry on business globally and must comply with GDPR and California privacy laws, it was easier to apply them to other jurisdictions rather than turning them on and off. In India, research participants who were aware of GDPR knew that it did not apply to their country; they wondered whether domestic companies intended to comply, especially when taken in conjunction with the Indian Supreme Court's 2017 Puttaswamy judgment, which reaffirmed privacy as a fundamental constitutional right in India. Participants were also confused about which data protection laws applied to them, and felt the burden was on them to understand applicability: "So if I can figure out which data protection laws apply to me, I can figure out what rights I've got" (P6, United States, on Alaska Air's privacy notice).

Even with the confusion about how laws might be relevant for people living in different places, the possibility that users could obtain their personal data from corporations could be empowering. After successfully requesting data from Google (but not Amazon), P15, from India, attempted to work through Flipkart's resistance to giving them data: "I pressed [the Flipkart representative] a little bit. I said, 'See, I tried it on Amazon and I got it. I tried it on Google and I got it.' At least Google by that time I'd already given the request, so I know it's possible. Amazon, I just simply told [Flipkart] that [Amazon gave me data]." Though unsuccessful, P15's experience with data controllers who complied with EU data laws shaped their expectations as to whether data controllers in India (Flipkart) should also comply with data access requests.

How to See the Nexus of Legal Code and Software Code

In this second part of the chapter, we have shown the nexus of legal and technical infrastructures that support rights of access in practice, which can only be seen through a bottom-up approach that focuses on the entire process by which law is implemented in practice. We have distilled much of this complexity in the simplified model of figure 3.1 to show how the law in action is a tangle of corporate and individual practices, business and personal motivations, and technical infrastructures. (The law in practice also includes how law is enforced in legal proceedings, in courts, and so forth and is not addressed in this chapter.)

On the "data supply" side, there is the company's technical infrastructure, wherein the legal framework is translated into actionable requests via software and code. On the "data demand" side is the personal technical

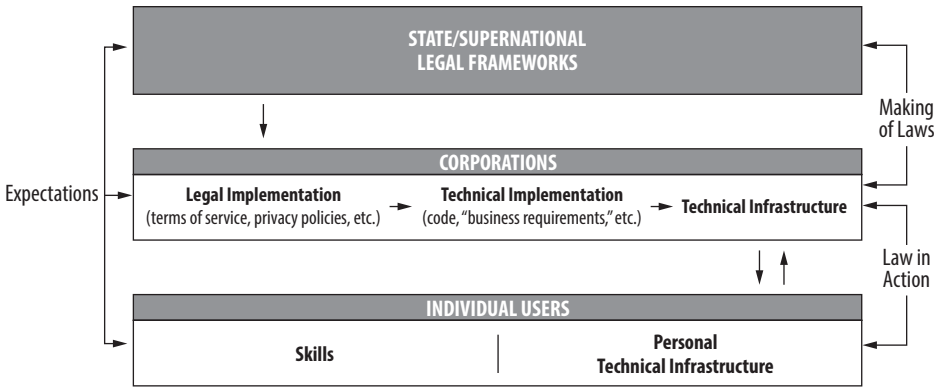

Figure 3.1. Provisional model of law in action for individual users acting in a private capacity.

infrastructure of data requesters, often a complex combination of various devices, software, and connectivity. There is also a wide variation in the (technical) personal skills that might be necessary to pursue the data requests and to open and interpret the files received. DSARs are the connective tissues between these two technical infrastructures and the wider influence of laws affecting data and the expectations they might engender (even if unfounded in law).

Conclusion

As we note in our opening to this chapter, in *An Engine, Not a Camera*, MacKenzie emphasized that the field actively transformed their object of study. As a tribute to this insight, we borrow a quote from one of our research participants for the chapter's title, "A Mirror, Not a Glass Door" and to show how companies, through their acquisition of personal data and control of data infrastructure, construct the conditions of data requests and data access:

> What I initially thought was a very powerful option, that GDPR . . . Oh my God. I know it's not like they can keep so much data about me. They have to show me what all they know about me. But, in fact, the way they're giving me data, clearly, it's like, they're holding a mirror to me. Yeah. So it's literally that right then what was supposed to be like a glass door that lets me see through what Google is doing with my data, instead of making this a glass door, they've just made it a mirror. They're like, oh, you want your data here? This is the data you gave me. They're just holding up a mirror to my face and saying, these are the data that you gave. This is not what this was. At least in my understanding, that's not what I expected. But I realized that that's what they're giving. So that is something that I find was an important thing. So there's still, whatever dump I've gotten leaves me no more intelligent than I was before I got this data. (P15, India, on Google data)

Our participants did not get the transparency that they expected data access would give them. As Waldman suggests, legal endogeneity in data protection laws can entrench corporate power over data by creating symbols of compliance that do little to achieve the emancipatory goals of data protection laws.

The metaphor of a mirror for personal data held by companies has been used before, with privacy researchers Ausloos and Dewitte observing that "data protection law and the values it aims to protect are but an illusion when assessed through a one-way mirror." "Shattering one way mirrors" can be done by aggregating collective experiences of exercising data rights.[55] But can these mirrors really be shattered by individuals who aim to find out how a company "sees" them through their data? Our work suggests that while aggregated assessment of data access requests could shatter mirrors, most people's experience remains that of looking in a one-way mirror.

Instead of a straightforward story about legal code regulating software code and producing particular results, the combination of software and legal code to enable personal data requests and access produced nondeterministic experiences for users because of variations in their personal computing infrastructure, individual expectations, and expertise (as indicated in figure 3.1). While the experience of our participants in attempting DSARs was mired in confusion and speculation, we also saw some glimpses of what Michael McCann calls "rights consciousness" as our participants interpreted their rights and asked for their data.[56]

Despite all of these confusions, our research provides evidence for trickledown GDPR: residents of India and the United States have personal data access rights for most instances when companies operate in the EU. Multinational corporations incorporate data privacy and protection laws into data infrastructures, extending the borders of legal regimes. A number of questions then emerge from our explorations of the variable experiences of trickledown GDPR: Are Indian and US residents experiencing a kind of European imperialism as EU rights are extended to contexts with different ideologies, cultures, and modes of data governance? Should we read trickledown GDPR as European values pushing back against the imperialism of dominant US technology firms? Have transnational companies empowered US and Indian residents with new rights? Does trickledown GDPR translate in other regions beyond those we examined? For example, China's new data protection laws were modeled on GDPR. Our experience shows that variation in the ways laws are implemented make it unlikely to be a universal experience, and the nuances are hard to predict with Chinese firms and require more research. As we have shown, moving from symbolic compliance into real protections cannot be done solely by examining legal and technical codes but must be grounded in people's actual experiences and goals.

Acknowledgments

We are grateful to Jef Ausloos for sharing research protocols and generous advice on designing this research project. Meg Leta Jones, Gerardo Con Díaz, and Jeff Yost provided important feedback on earlier drafts of this chapter. Meg Young helped pilot research protocols. This research was supported by the University of Washington Information School's Strategic Research Fund.

Notes

1. In 2023 India passed the Digital Personal Data Protection Act.

2. Anu Bradford, "The Brussels Effect," *Northwestern University Law Review* 107, no. 1 (Fall 2012): 1–67, https://scholarlycommons.law.northwestern.edu/nulr/vol107/iss1/1; Anupam Chander, Margot Kaminski, and William McGeveran, "Catalyzing Privacy Law," *Minnesota Law Review* 105 (2021): 1736–1802, https://minnesotalawreview.org/wp-content/uploads/2021/04/3-CKM_MLR.pdf.

3. Donald MacKenzie, *An Engine, Not a Camera: How Financial Models Shape Markets* (Cambridge, MA: MIT Press, 2006), 12,

4. General Data Protection Regulation (GDPR), Article 4(1).

5. Viktor Mayer-Schönberger, "Generational Development of Data Protection in Europe," in *Technology and Privacy: The New Landscape*, *ed. Philip E. Agre and Marc Rotenberg* (Cambridge: MA: MIT Press, 1998).

6. Philip L. Frana, "Telematics and the Early History of International Digital Information Flows," *IEEE Annals of the History of Computing* 40, no. 2 (April 2018): 32–47, https://doi.org/10.1109/MAHC.2018.022921442.

7. Frana, "Telematics," 41.

8. Sandra Braman, "Vulnerabilities of the State and the New World Information and Communication Order," *Media Development*, no. 3 (1991): 3; Miriyam Aouragh and Paula Chakravartty, "Infrastructures of Empire: Towards a Critical Geopolitics of Media and Information Studies," *Media, Culture, and Society* 38, no. 4 (May 1, 2016): 559–75, https://doi.org/10.1177/0163443716643007.

9. Frana, "Telematics"; Armand Mattelart, *The Information Society: An Introduction*, trans. Susan G. Taponier and James A. Cohen (London: Sage, 2003); Fred Turner, *From Counterculture to Cyberculture* (Chicago: University of Chicago Press, 2006).

10. The history of data protection legislation in the United Kingdom is both distinct and entwined with that in the EU. In the United Kingdom, the debate on privacy and data protection started early with a number of private members' bills introduced in the House of Commons and in the House of Lords from 1961 to 1972 without being passed into law. The 1972 report of the Committee on Privacy recommended against a general privacy law, but a section of the report dealt with the collection and handling by computers of personal information, and possible misuse. It recommended 10 principles for the use of personal data by computers, which included specifying the purpose of holding data, giving subject access to data, and keeping data accurate, up-to-date, and for limited periods. It took until 1984, however, for the government to enact the Data Protection Act, which focused on data automatically processed, rather than on the right to privacy. Adam Warren and James Dearnley, "Data Protection Legislation in the United Kingdom: From Development to Statute, 1969–84," *Information, Community, and Society* 8, no. 2 (2005): 238–63. The right to privacy became part of the 1998 Data Protection Act, which enacted the EU Data Protection Directive of 1995. The 1998 act was replaced by the 2018 Data Protection

Act, which enacted the EU GDPR in the United Kingdom. Although the United Kingdom left the EU in 2020, it retained the UK GDPR. See the "Overview—Data Protection and the EU," ICO: Information Commissioner's Office (UK), accessed February 3, 2025, https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/.

11. Mayer-Schönberger, "Generational Development of Data Protection in Europe."

12. Meg Leta Jones and Margot E. Kaminski, "An American's Guide to the GDPR," *Denver Law Review* 98, no. 1 (2021): 111, https://papers.ssrn.com/abstract=3620198.

13. Jones and Kaminski, "An American's Guide to the GDPR."

14. Jef Ausloos and Pierre Dewitte, "Shattering One-Way Mirrors: Data Subject Access Rights in Practice," *International Data Privacy Law* 8, no. 1 (February 1, 2018): 7 (emphasis ours), https://doi.org/10.1093/idpl/ipy001.

15. Clive Norris, Paul de Hert, Xavier L'Hoiry, and Antonella Goletta, eds., *The Unaccountable State of Surveillance: Exercising Access Rights in Europe*, Law, Governance and Technology Series (Cham, Switzerland: Springer International, 2017), 5, https://doi.org/10.1007/978-3-319-47573-8_1.

16. Jan Philipp Albrecht, *Hands Off Our Data!* (Strasbourg: Greens / European Free Alliance in the European Parliament, 2015; René Mahieu and Jef Ausloos, "Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access," Law Archive, July 2, 2020, https://doi.org/10.31228/osf.io/b5dwm.

17. For extensive discussion of the shift away from projects such as the National Data Center, the Ware reports on the 1970s, and the 1974 Privacy Act toward the commercialization of the internet under the Clinton administration, see Meg Leta Jones, *The Character of Consent: The History of Cookies and the Future of Technology Policy* (Cambridge, MA: MIT Press, 2024); Dan Bouk, "The National Data Center and the Rise of the Data Double," *Historical Studies in the Natural Sciences* 48, no. 5 (November 1, 2018): 627–36, https://doi.org/10.1525/hsns.2018.48.5.627; Christopher Loughnane and William Aspray, "Rethinking the Call for a US National Data Center in the 1960s: Privacy, Social Science Research, and Data Fragmentation Viewed from the Perspective of Contemporary Archival Theory," *Information and Culture* 53, no. 2 (May 2018): 203–42, https://doi.org/10.7560/IC53204; Robert Waterman McChesney, *Digital Disconnect: How Capitalism Is Turning the Internet against Democracy* (New York: The New Press, 2013); Paul M. Schwartz and Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law," *Georgetown Law Journal* 106 (2017): 137, https://works.bepress.com/paul_schwartz/71/; Willis H. Ware, "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security" (Santa Monica, CA: RAND Corp., February 1970); Fred H. Cate, "The Failure of Fair Information Practice Principles," in *Consumer Protection in the Age of the Information Economy*, ed. Jane K. Winn, Markets and the Law (London: Routledge, 2006).

18. Daniel J. Solove, "Privacy Self-Management and the Consent Dilemma," *Harvard Law Review* 126 (2013): 1880–1903; Julie Brill, "Remarks by Commissioner Julie Brill—Privacy 3.0 Panel," presented at Conference of Western Attorneys General Annual Meeting, Santa Fe, NM, July 20, 2010, https://www.ftc.gov/public-statements/2010/07/presentation-commissioner-julie-brill.

19. Julie E. Cohen, "What Privacy Is For," in "Symposium: Privacy and Technology," *Harvard Law Review*, 126, no. 7 (2013): 1904–33, https://harvardlawreview.org/wp-content/uploads/2013/05/vol126_cohen.pdf; Alessandro Acquisti et al., "Nudges for Privacy and Security: Understanding and Assisting

Users' Choices Online," *ACM Computing Surveys* 50, no. 3 (August 8, 2017): 44:1–41, https://doi.org/10.1145/3054926.

20. Schwartz and Peifer, "Transatlantic Data Privacy Law," 150–55; Lon L. Fuller, *Legal Fictions*, Notations edition (Stanford, CA: Stanford University Press, 1967); Solove, "Privacy Self-Management and the Consent Dilemma."

21. Chander, Kaminski, and McGeveran, "Catalyzing Privacy Law."

22. Cal. Civ. Code §1798.115; Va. Code § 59.1-573(A).

23. Graham Greenleaf, "GDPR-Lite and Requiring Strengthening—Submission on the Draft Personal Data Protection Bill to the Ministry of Electronics and Information Technology (India)," UNSW (University of New South Wales) Law Research Paper No. 18-83, September 20, 2018, http://dx.doi.org/10.2139/ssrn.3252286.

24. Justice K. S. Puttaswamy (Retd) v. Union of India on 26 September, 2018, Indian Kanoon, https://indiankanoon.org/doc/127517806/

25. Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, Government of India, 2018), 10, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

26. Greenleaf, "GDPR-Lite and Requiring Strengthening—Submission on the Draft Personal Data Protection Bill."

27. Section 8(1)(j) of the RTI Act, 2005, currently reads as follows: "8(1) Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen: (j) information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information." Section 44(3) of the Digital Personal Data Protection Act of 2023 replaces clause 8(1)(j) with: "information which relates to personal information."

28. For critiques of the 2019 draft by the drafters themselves of the Srikrishna Committee report, see Megha Mandavia, "Personal Data Protection Bill Can Turn India into 'Orwellian State': Justice BN Srikrishna," *Economic Times* (Mumbai, updated December 19, 2019, https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turnindia-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms; and Rahul Nair, "The Personal Data Protection Bill, 2019: A Constitutional Critique," Constitutional Law and Philosophy (blog), January 8, 2020, https://indconlawphil.wordpress.com/2020/01/08/the-personal-date-protection-bill-2019-a-constitutional-critique/. For critiques of the current (2023) act, see Rashmi Rajagopal, "New Data Protection Law Draws Criticism," *Deccan Herald* (Bengaluru, India), updated August 15, 2023, https://www.deccanherald.com/india/karnataka/bengaluru/new-data-protection-law-draws-criticism-2648820; and Gayatri Malhotra, "India's Data Protection Law Does Little for Privacy while Bolstering the State's Surveillance Powers," *Scroll*, September 26, 2023. For critiques of the draft rules published in January 2025, see Aaratrika Bhaumik, "Draft Data Protection Rules: What Are the Concerns Related to Localisation Norms and Government Exemptions?" *The Hindu*, January 16, 2025, https://www.thehindu.com/news/national/draft-data-protection-rules-what-are-the-concerns-related-to-localisation-norms-and-government-exemptions/article69094728.ece; and the Internet Freedom Foundation's statement of January 4, 2025, https://internetfreedom.in/statement-on-the-draft-dpdp-rules-2025/.

29. Subhashis Banerjee, "Short on Nuance: Draft Data Protection Bill Has Lost Sight of The Intricacies of Digital Identity," *Indian Express* (Mumbai), December 6, 2018, https://indianexpress.com/article/opinion/columns/aadhaar-data-protection-bill-privacy-cambridge-analytica-5480398/; Smriti Parsheera, "Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?" Data Governance Network Working Paper 5, December 5, 2019, https://ssrn.com/abstract=3525324 or http://dx.doi.org/10.2139/ssrn.3525324; Vidushi Marda, "Every Move You Make," *India Today*, November 29, 2019, https://www.indiatoday.in/magazine/up-front/story/20191209-every-move-you-make-1623400-2019-11-29.

30. For a critique of the bill before its passage as an act that pertains to its effect on the RTI, see "'Regressive Amendments to RTI Act': NCPRI Flags Concerns over Digital Personal Data Protection Bill," *The Wire*, August 4, 2023, https://thewire.in/rights/regressive-amendments-to-rti-act-ncpri-flags-concerns-over-digital-personal-data-protection-bill. For a discussion of the act after it was passed, see M. Sridhar Acharyulu, "How the 'Strict' Data Act Is Diluting RTI," *Down to Earth*, September 8, 2023.

31. D. Graham Burnett, *Trying Leviathan: The Nineteenth-Century New York Court Case That Put the Whale on Trial and Challenged the Order of Nature* (Princeton, NJ: Princeton University Press, 2007), 196.

32. Regarding IBM, see, for example, Corinna Schlombs, "Engineering International Expansion: IBM and Remington Rand in European Computer Markets," *IEEE Annals of the History of Computing* 30, no. 4 (October 2008): 42–58, https://doi.org/10.1109/MAHC.2008.66; Eden Medina, "Big Blue in the Bottomless Pit: The Early Years of IBM Chile," *IEEE Annals of the History of Computing* 30, no. 4 (October 2008): 26–41, https://doi.org/10.1109/MAHC.2008.62; Colette Perold, "IBM's World Citizens: Valentim Bouças and the Politics of IT Expansion in Authoritarian Brazil," *IEEE Annals of the History of Computing* 42, no. 3 (July 2020): 38–52, https://doi.org/10.1109/MAHC.2020.3010892.

33. Bradford, "Brussels Effect."

34. Paul M. Schwartz, "Global Data Privacy: The EU Way," New York University Law Review 94, no. 4 (October 2019), https://nyulawreview.org/issues/volume-94-number-4/global-data-privacy-the-eu-way/.

35. Nora McDonald and Andrea Forte, "The Politics of Privacy Theories: Moving from Norms to Vulnerabilities," in *CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, April 25–30, 2020, Honolulu, HI* (New York: Association for Computing Machinery, 2020), 1–14, https://doi.org/10.1145/3313831.3376167; Payal Arora, "Decolonizing Privacy Studies," *Television and New Media* 20, no. 4 (May 2019): 366–78, https://doi.org/10.1177/1527476418806092.

36. See, for example, Syed Ishtiaque Ahmed, Md. Romael Haque, Irtaza Haider, Jay Chen, and Nicola Lee Dell, "'Everyone Has Some Personal Stuff': Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh," in *CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (New York: Association for Computing Machinery, 2019), 1–13, https://doi.org/10.1145/3290605.3300410; Rishabh Bailey, Smriti Parsheera, Faiza Rahman, and Renuka Sane, "Disclosures in Privacy Policies: Does 'Notice and Consent' Work?," National Institute of Public Finance and Policy Working Paper 246, December 11, 2018; Seeta Peña Gangadharan, "The Downside of Digital Inclusion: Expectations and Experiences of Privacy and Surveillance among Marginal Internet Users," *New Media and Society* 19, no. 4 (April 2017): 597–615, https://doi.org/10.1177/1461444815614053; Margaret C. Jack, Pang Sovannaroth, and Nicola Dell, "'Privacy Is Not a Concept, but a Way of Dealing

with Life': Localization of Transnational Technology Platforms and Liminal Privacy Practices in Cambodia," *Proceedings of the ACM on Human-Computer Interaction* 3, issue CSCW (November 7, 2019): 1–19, https://doi.org/10.1145/3359230.

37. Janaki Srinivasan et al., "The Poverty of Privacy: Understanding Privacy Trade-Offs from Identity Infrastructure Users in India," *International Journal of Communication* 12 (March 1, 2018): 20, https://ijoc.org/index.php/ijoc/article/view/7046.

38. Jones and Kaminski, "An American's Guide to the GDPR," 116.

39. Jones and Kaminski, "An American's Guide to the GDPR," 111; Margot E. Kaminski, "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability," *Southern California Law Review* 92, no. 6 (2019): 1529, https://doi.org/10.2139/ssrn.3351404.

40. Norris, *Unaccountable State of Surveillance*, 5. On border-crossing materials and policy, see Emilie Cloatre and Robert Dingwall, " 'Embedded Regulation:' The Migration of Objects, Scripts, and Governance," *Regulation and Governance* 7, no. 3 (2013): 365–86, https://doi.org/10.1111/j.1748-5991.2012.01152.x.

41. For a discussion of material representations of patent law, see Alain Pottage and Brad Sherman, *Figures of Invention: A History of Modern Patent Law* (Oxford: Oxford University Press, 2010).

42. Schwartz, "Global Data Privacy"; Schwartz and Peifer, "Transatlantic Data Privacy Law"; Bradford, "Brussels Effect"; Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, and Ignacio Sanchez, "The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services," *Computer Law and Security Review* 34, no. 2 (April 2018): 193–203, https://doi.org/10.1016/j.clsr.2017.10.003; Bert-Jaap Koops and Ronald Leenes, "Privacy Regulation Cannot Be Hardcoded: A Critical Comment on the 'Privacy by Design' Provision in Data-Protection Law," *International Review of Law, Computers, and Technology* 28, no. 2 (May 4, 2014): 159–71, https://doi.org/10.1080/13600869.2013.801589.

43. Margot E. Kaminski and Gianclaudio Malgieri, "Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations," *International Data Privacy Law* 11, no. 2 (April 2021): 125–44, https://doi.org/10.1093/idpl/ipaa020.

44. See, for example, De Hert et al., "The Right to Data Portability in the GDPR"; Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz, "The Privacy Policy Landscape after the GDPR," *Proceedings on Privacy Enhancing Technologies* 2020, no. 1 (January 7, 2020): 47–64, https://doi.org/10.2478/popets-2020-0004; Janis Wong and Tristan Henderson, "How Portable Is Portable? Exercising the GDPR's Right to Data Portability," in *UbiComp '18: Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers* (Singapore: Association for Computing Machinery, 2018), 911–20, https://doi.org/10.1145/3267305.3274152; Luca Bufalieri, Massimo La Morgia, Alessandro Mei, and Julinda Stefa, "GDPR: When the Right to Access Personal Data Becomes a Threat," paper presented at 2020 IEEE International Conference on Web Services (ICWS), Beijing, October 19–23, IEEE Xplore, December 2020, https://doi.org/10.1109/ICWS49710.2020.00017; Jatinder Singh and Jennifer Cobbe, "The Security Implications of Data Subject Rights," *IEEE Security Privacy* 17, no. 6 (November 2019): 21–30, https://doi.org/10.1109/MSEC.2019.2914614.

45. Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (Cambridge: Cambridge University Press, 2021), 102.

46. Lauren B. Edelman, *Working Law: Courts, Corporations, and Symbolic Civil Rights*, Chicago Series in Law and Society (Chicago: University of Chicago Press, 2016), https://doi.org/10.7208/9780226400938.

47. Gerardo Con Díaz, *Software Rights: How Patent Law Transformed Software Development in America* (New Haven, CT: Yale University Press, 2019), https://yalebooks.yale.edu/book/9780300228397/software-rights.

48. Norris et al., *Unaccountable State of Surveillance*; Lokman Tsui and Stuart Hargreaves, "Who Decides What Is Personal Data? Testing the Access Principle with Telecommunication Companies and Internet Providers in Hong Kong," *International Journal of Communication* 13 (2019): 15; Tobias Urban et al., "Measuring the Impact of the GDPR on Data Sharing in Ad Networks," in *ASIA CCS '20: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security* (New York: Association for Computing Machinery, 2020), 222–35, https://doi.org/10.1145/3320269.3372194.

49. Alaska Airlines did business outside the United States but had no direct flights to EU member states at the time this research was conducted.

50. Ausloos and Dewitte, "Shattering One-Way Mirrors."

51. Clayton Lewis, "Using the 'Thinking-Aloud' Method in Cognitive Interface Design," IBM Thomas J. Watson Research Center, Yorktown Heights, NY, February 17, 1982, https://dominoweb.draco.res.ibm.com/reports/RC9265.pdf; K. Anders Ericsson and Herbert A. Simon, "Verbal Reports as Data," *Psychological Review* 87, no. 3 (May 1980): 215–51, https://doi.org/10.1037/0033-295X.87.3.215.

52. Chander, Kaminski, and McGeveran, "Catalyzing Privacy Law."

53. Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society* 4, no. 3 (2008): 543–68, https://heinonline.org/HOL/P?h=hein.journals/isjlpsoc4&i=563.

54. Jones and Kaminski, "An American's Guide to the GDPR."

55. Ausloos and Dewitte, "Shattering One-Way Mirrors."

56. Michael W. McCann, *Rights at Work: Pay Equity Reform and the Politics of Legal Mobilization*, Chicago Series in Law and Society (Chicago: University of Chicago Press, 1994), https://press.uchicago.edu/ucp/books/book/chicago/R/bo3630053.html. McCann defines "rights consciousness" as "the ongoing, dynamic process of constructing one's understanding of, and relationship to, the social world through use of legal conventions and discourses" (7).

Contributors

Jennifer Alexander is an Associate Professor in Mechanical Engineering at the University of Minnesota, where she is the Director of Graduate Studies for the Program in the History of Science, Technology, and Medicine.

Héctor Beltrán is an Associate Professor of Anthropology at the Massachusetts Institute of Technology. He is the author of *Code Work: Hacking across the US/México Techno-Borderlands* (Princeton University Press, 2023).

Shun-Ling Chen is an Associate Research Professor and the Codirector of the Information Law Center at Institutum Iurisprudentiae, Academia Sinica.

Gerardo Con Díaz is a Professor of Science and Technology Studies at the University of California, Davis. He is the author of *Everyone Breaks These Laws: How Copyrights Made the Online World* (Yale University Press, 2025) and *Software Rights: How Patent Law Transformed Software Development in America* (Yale University Press, 2019).

Stephanie Dick is an Assistant Professor in the School of Communication at Simon Fraser University. Her work explores the history of mathematics, computing, and the mind in the postwar United States.

Hamid R. Ekbia is a University Professor and the Director of the Autonomous Systems Policy Institute at the Maxwell School of Citizenship and Public Affairs, Syracuse University.

Megan Finn is an Associate Professor in the School of Communication at American University and an Affiliate Associate Professor in the Information School at the University of Washington. She is the author of *Documenting Aftermath: Information Infrastructures in the Wake of Disasters* (MIT Press, 2018).

Mar Hicks is a historian of technology and an Associate Professor of Data Science at the University of Virginia, Charlottesville. Hicks is the author of *Programmed Inequality* (MIT Press, 2017) and a coeditor of *Your Computer Is on Fire* (MIT Press, 2021).

Ya-Wen Lei is a Professor in the Department of Sociology at Harvard University. She is also affiliated with the Fairbank Center for Chi-

nese Studies and the Weatherhead Center for International Affairs at Harvard.

Mariel García Llorens is an anthropologist and scholar of science and technology studies who researches digital money in Latin America. She holds a PhD from the University of California, Davis.

A. P. Janani was an MSc (Digital Society) student at the International Institute of Information Technology Bangalore at the time that the research for chapter 3 was conducted.

Meg Leta Jones is a Provost's Distinguished Associate Professor for the Master's in Communication, Culture & Technology Program at Georgetown University, where she researches rules and technological change with a focus on computers and privacy.

Shreeharsh Kelkar is a Continuing Lecturer in Interdisciplinary Studies at the University of California, Berkeley, and is currently working on a manuscript about the practices and politics of data science.

Dylan Mulvin is an Associate Professor of Media and Communications at the London School of Economics and Political Science.

Nico Wen-Li Ong is a research intern and editorial assistant for Gerardo Con Díaz at the University of California, Davis, and helped the coeditors prepare this book for production.

Elisa Oreglia is a Reader in Global Digital Cultures at King's College London.

Justin Petelka is a PhD candidate at the University of Washington's Information School and a Cybersecurity Fellow of the International Policy Institute at the University of Washington's Henry M. Jackson School of International Studies.

Elizabeth Petrick is an Associate Professor of History at Rice University and the author of *Making Computers Accessible: Disability Rights and Digital Technology* (Johns Hopkins University Press, 2015).

Elizabeth Semler is a historian of science, medicine, and technology at the University of California, Berkeley, Library's Oral History Center.

Janaki Srinivasan is an Associate Professor of Digital South Asian Studies at the University of Oxford. At the time that research for chapter 3 was conducted, she was on the faculty at the International Institute of Information Technology Bangalore.

Gili Vidan is an Assistant Professor in the Department of Information Science of the Cornell Bowers College of Computing and Information Science and a field member in Cornell University's Department of Science and Technology Studies and the Media Studies Program.

Jeffrey R. Yost is the Director of the Charles Babbage Institute and Research Professor of the History of Science, Technology, and Medicine at the University of Minnesota. He has published eight books, including *Making IT Work: A History of the Computer Services Industry* (MIT Press, 2017).