The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

Chapter 9

Governing Data

The information-imperium state has emerged through a series of fundamental social, economic, political and technological shifts. Chapters 5 through 8 examined how these shifts are transforming the ways in which state and private actors understand, value and have incorporated data into their activities, and how this incorporation has reshaped the exercise of power. Reflecting upon those chapters, this chapter asks: Which actors have the legitimacy and authority to determine what types of data should be collected, the manner in which that data can be legitimately used and the appropriate modes of data governance? In short, who can and, more importantly, who *should* set the rules of data governance that are at the heart of structural power in the knowledge-driven society? Whose interests should be served by this regime, and how might they affect data governance?

The starting point for this chapter is the recognition that the information-imperium state is highly contested. As we've set out in the book, knowledge feudalism and digital economic nationalism are the two opposing economic strategies within the information-imperium state. The United States, the dominant knowledge-feudalist actor, prioritizes global flows of data and the maximalist protection for intellectual property rights, which largely benefit US industry. The United States also has economic, political and national security interests in ensuring the free flow of data globally, and its large data companies disproportionately benefit from capturing, interpreting and monetizing these data flows. As a counterpoint to knowledge feudalism, multiple states are undertaking various digital economic nationalist strategies, including policies that restrict or regulate global flows of data. These include policies that require data to be stored within a state's legal jurisdiction, a practice termed 'data sovereignty' that this chapter explores.

Haggart and Tusikov_9781538160879.indb 223 31-05-2023 17:08:52

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

The European Union, the most prominent digital economic nationalist actor alongside China, capitalizes upon its large internal market and regulatory capacity to institute its own preferred rules on the data market. This chapter explores how the EU's General Data Protection Regulation (GDPR), widely perceived as a global data-protection standard, regulates but does not dismantle the problematic trade in personal data. We contend that the GDPR must be understood as part of the European Union's long-term strategy to become a global regulatory superpower, exporting its preferred data standards and practices to other countries and applying them to big data actors, including US companies like Apple and Facebook. In the terminology of this book, the European Union is aspiring to become a knowledge feudalist by setting rules for the market in personal data that are applied globally through the extraterritorial application of the GDPR.

In staunch opposition to an information-imperium state that accords economic, political and social power to the control over knowledge, there exists a collective rights approach that centres human rights within the knowledge structure. This approach encompasses an array of strategies and practices, and brings together a diverse coalition of workers, activists, civil-society groups, privacy experts and technologists, and Indigenous groups. While opposition takes many forms, common amongst them is resistance to the surveillance-intensive practices of governments and businesses, as well as pushback against dataist ideologies that privilege quantifying all aspects of human life and employ automated data techniques to augment or even replace human decision-making. A human rights approach tends to favour restrictions on the collection and use of personal data, particularly its commodification, and to support data-governance models that accord greater collective control rather than corporate models that focus on narrow commercial interests. In a rejection of the dataist imperative that all data must have value extracted to realize social and economic benefits, some actors within the human rights approach advocate for people to have the right to exit data markets, essentially opting out of corporate practices datafying all aspects of social life. In contrast to knowledge feudalism and digital economic nationalism, we term this approach 'data decommodification'.

Workers and citizens, for example, are engaging in protests against surveillance-focused business models that exist to monetize data. Such efforts are particularly evident in the exploitative gig economy, where workers have sued gig companies to be recognized as employees and engaged in strikes and other collective labour action (Woodcock and Graham 2020). Resistance is also evident against the intensification of state security–related surveillance programmes (e.g., Stevens and Allen-Robertson 2021), as well as protests and lawsuits against state use of automated tools to manage and deliver public services like welfare (Vervloesem 2020).

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

While contestation can be seen at the state level, it is also present within the knowledge-driven society itself. This contestation is focused not just on the ability to reap the spoils of the knowledge-driven society, but on the meaning of fundamental terms, like privacy. While this book has explored the tendencies, or imperatives, of the information-imperium state toward pervasive surveillance and knowledge commodification in pursuit of improved security and boosting economic growth, data and knowledge governance remain contested topics, including both their meaning and their limits.

This chapter reflects upon the contested state of data governance. Alongside efforts to scale back corporate and state surveillance measures, scholars and activists are developing concepts that emphasize collective approaches in the treatment of data and human rights more broadly to counter the hegemony of the information-imperium state. Collective data-governance approaches – data justice, group privacy and Indigenous data sovereignty – emphasize governance by and benefits accruing to a collective in contrast to legal frameworks focused on individual control and individual rights, while also generally pushing back against the commodification of data.

This chapter proceeds in four sections. First, it argues for the need for a critical rethinking of individualized notions of privacy and consent. As part of this consideration, we explore how the EU's GDPR functions not only as a regulation to standardize the treatment of personal data across Europe but also as part of the EU's efforts to shape regulations globally that prioritize its own particular economic and social interests, which may not align with the interests and needs of others. The chapter argues that we need alternative human rights approaches to privacy and to data governance more broadly to counter the problems inherent in the data economy, principally pervasive surveillance, discriminatory data practices and vast gulfs between those accumulating power through knowledge and those without such power.

Second, the chapter examines forms of resistance to the information-imperium state by considering various collective models of data governance, including data trusts and data sovereignty approaches, particularly Indigenous data sovereignty. Third, the chapter considers the concepts of group privacy and data justice as human rights-centred alternatives to the problems of an increasingly datafied society and economy. The chapter ends with a brief conclusion.

RETHINKING PRIVACY AND CONSENT

Understandings of privacy are neither unchanging nor universal. Underlying the global data economy is the Western individual-focused understanding

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

of privacy that draws from the Anglo-Saxon legal tradition. Privacy is understood to be an individual right similar to other individualized notions of human rights (Taylor et al. 2017b). This individualized conception of privacy is evident in companies' legal terms-of-service agreements, which require all users to signal their consent (say, by clicking 'I agree' on a website) before being able to access digital products and services. As explained in chapter 4, understanding privacy as attached to individuals has been the dominant view since the late 1990s, exported globally from the United States through its tech companies via the so-called notice-and-consent model of privacy policies (Cranor 2012, 304), a practice that has enabled the United States to become a knowledge-feudalist state. This model of privacy assumes that people are capable of acting as rational consumers who read and understand the policies (notice) and then give informed consent (choice) (Cranor 2012). The model, which provides the legal underpinning of the digital economy, problematically assumes that privacy can be straightforwardly understood as applying to the collection and use of personally identifiable information.

Understanding Privacy and Consent

Privacy is a more complex and intangible concept than is generally acknowledged. 'There is no overarching conception of privacy', explains privacy scholar Daniel Solove (2008, x): 'it must be mapped like terrain, by painstakingly studying the landscape'. A perennial challenge with privacy is that it is 'an unusually slippery concept' (Whitman 2004, 1153), as what is considered to be 'private', such as public nudity, varies widely among societies and over time, as do state regulatory frameworks and private-sector data practices. There are gender, race and class dimensions to how people experience privacy, dependent upon their status and circumstances. Historically, institutionalized populations, including prisoners, and noncitizens, immigrants, children, people with disabilities, and racial and sexual minorities have been disproportionately subjected to intensive bureaucratic surveillance, a trend that continues today (see Igo 2018). Similarly, women and sexual minorities traditionally were presumed to have a lesser claim on privacy than heterosexual men (Igo 2018, 9). Concerns about state and corporate limitations on and violation of individual and groups' privacy are nothing new, as historian Sarah Igo (2018) explores in her historical study of shifts in public understandings of privacy in the United States following the US government's introduction of its social insurance programme that provides retirement benefits. While many studies traditionally focused on privacy rights in relation to governmental practices, privacy in relation to private-sector activities has become an increasingly important topic (for an early influential text, see Gandy 1993).

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

Consent, like privacy, is a more complicated concept than it may first appear. Key to understanding consent is the idea of informed consent. Generally, consent is seen as valid only when people can understand to what they are consenting and are given clear options to accept or decline the data collection, use or disclosure (see e.g., Hoofnagle 2018). The EU's GDPR, for example, defines 'informed' consent as a 'freely given, specific, informed and unambiguous indication' or 'a clear affirmative action' (European Parliament 2016 GDPR Art. 4(11)). In some cases, however, there may be no way to opt out, if the data collection is attached to critical services like transit or when data collection is tied to locations in a smart city.

Recognizing that most people do not read terms-of-service agreements, legal scholar Teresa Scassa (2018a) argues that 'clicking "I agree" without reading privacy policies is an act of surrender, not of consent'. Communication scholar Jonathan Obar (2015, 2) concludes that this situation reflects 'the fallacy of data privacy self-management', in reference to the misconception that people can understand and provide informed consent in this area. Companies' practice of unilaterally changing the terms of the agreements without notice to the user can result in 'shadow terms', which consumers may not know about (Horton 2010). People cannot consent to future uses of their data of which they are unaware, and it is nearly impossible for ordinary people to calculate a fair or reasonable exchange of services for personal data. Implicit within the model of informed consent is the idea that consumers can decline contracts with onerous conditions, if they are aware of them, or they can switch to providers with more favourable conditions. Switching providers, however, can impose costs, assuming that there are even viable alternatives. This, unfortunately, is not the case in many parts of the winner-take-most data-driven economy. Social media companies, for example, almost all operate with similar surveillance-based business models, while it is difficult to find non-smart versions of many consumer goods like televisions.

The lack of informed consent in terms-of-service contracts can lead to negative outcomes for users. Contracts may, for instance, 'restructure the rights of users' or, even more worrisome, 'delete rights that are granted through democratic processes, substituting for them the system that the firm wishes to impose' (Radin 2012, 16). This problem can be evident in contracts deployed internationally by globally dominant companies with little regard for the distinctive nature of domestic legal systems. Legal wording that may have been drafted to respond to the needs, ideologies and requirements of one jurisdiction (usually the United States) ends up being exported to other jurisdictions, like Australia, to the extent of reproducing 'verbatim the contractual wording of the original US source' even though the language may not be suitable (Noto La Diega and Walden 2016, 3). As a result, legal contracts attached to digital services or software-enabled products are 'commonly'

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

used within Australian contracts even when not particularly suitable (Manwaring 2017, 286). This cookie-cutter approach, discussed in chapter 7 in relation to agricultural data, has the effect that consumers, typically those in smaller countries, are subject to rules set in another country. These practices of rule exportation raise classic questions of regulatory scope and legitimacy: Whose rules and where?

The GDPR: Not a Privacy 'Gold Standard'

Given the challenges outlined earlier with how we understand privacy and consent-based data collection, solutions can be difficult to articulate. A common – and understandable – reaction to the ills of the data-driven economy is a call for new or strengthened data-protection laws, including tougher privacy measures. For many privacy scholars and privacy-focused policymakers, the EU's General Data Protection Regulation (GDPR), which came into force in May 2018, offered a groundbreaking development in terms of privacy protection. The GDPR does more than just enact data-protection and privacy rules on the personal data across the European Union. Crucially, it is designed to regulate, not impede, the trade in personal data (Daly 2021), while also enabling the European Union to exert global structural power by setting global standards for the online treatment of personal data (Bradford 2020). In its attempt to set global standards for the data market, the European Union is endeavouring to become a knowledge-feudalist state.

Advocates of the GDPR claim it constitutes 'a sort of digital gold standard' and 'the most ambitious endeavour so far to secure the rights of the individual in the digital realm for a generation' (Buttarelli 2016, 78, 77). The GDPR harmonizes privacy laws throughout the European Union in relation to the collection and processing of EU residents' personal data, which includes mining, aggregating and sharing data. It applies to entities, whether in the European Union or outside, that collect data from EU residents in relation to offering goods or services to Europeans or monitoring their behaviour. Amongst its key provisions, the GDPR sets out a stricter definition of consent and new rights for individuals to access their data. With some exceptions, EU residents can erase their data, restrict the processing of personal data and have the right to data portability, which means that people can transfer their personal data from one entity to another.[1]

Following the introduction of the GDPR, multiple countries have adopted or are in the process of introducing data-protection laws. Brazil, long considered a leader in digital rights following the passage of its *Marco Civil da Internet* (Bill of Rights for the Internet) in 2014, introduced its *General Personal Data Protection Law* (LGPD) in 2018 and created a National Data

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

Protection Authority (ANPD) in 2020. Although the United States lacks GDPR-like provisions at the federal level, California passed its 2018 *Consumer Privacy Act*. Countries in Africa, Asia and Latin America have adopted GDPR-like data provisions, in part to ensure continued access to the European Union's market (Bradford 2020). While each of these state efforts can be understood as digital economic nationalist responses, that these laws are intended to complement the GDPR to enable access to the European market demonstrates the regulatory power of the European Union.

Although the GDPR is rightly praised for establishing a baseline of data protection, it should not be understood as a bulwark against the pervasive surveillance characteristic of the digital economy. The GDPR was designed to facilitate data collection and streamline digital capitalism across the European market, particularly in terms of the trade in personal data. After all, the European Union, like other states and regions, needs a functioning data economy, and there is an additional need in Europe for consistency in the treatment of personal data across EU Member States. The GDPR is a digital economic nationalist response that endeavours to balance principles of freedom, security and economic development according to European preferences in contrast to the free-market orientation of the United States.

Legal scholar Angela Daly (2021, 88) contends that the GDPR is 'ultimately permissive of various surveillance capitalist data gathering and processing practices' as it sets out rules for the datafication of personal data. This is because the GDPR facilitates 'the free flow of personal data between Member States' (Article 3). The effect, Daly argues, is that instead of countering surveillance capitalism, the GDPR is effectively establishing a 'surveillance capitalist Internet with European characteristics' with those characteristics being stronger data-protection compliance and oversight than elsewhere (Daly 2021, 92–93). In essence, the GDPR has a dual aim as a digital economic nationalist strategy: it establishes important data-protection standards for all EU residents and ensures the free flow of personal data throughout the European Economic Area.

Consequently, the GDPR regulates the digital economy but does little to curb the trade in personal data. More broadly, the GDPR enables the European Union to reach its long-standing ambition of becoming a regulatory superpower on the global stage in two ways. First, the GDPR applies extraterritorially to govern non-European actors that collect data on EU residents (like a Canadian company selling products to Europeans). Second, other countries are adopting provisions similar to the GDPR to be able to continue trading with the European Union. This is why the GDPR functions as more than a data-protection law: it is a key part of the European Union's long-standing effort to establish itself as a regulatory superpower.

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

EU as Regulatory Superpower

The EU's GDPR is more than just an EU law. It is an example of the 'Brussels Effect' that we discussed in chapter 8, the European Commission's practice of strategically exporting its preferred standards globally (Bradford 2020). The GDPR has a similar extraterritorial application, requiring all companies serving EU residents, even those located outside Europe, to institute GDPR rules in the treatment of personal data. Companies and states outside the European Union thus have a strong interest in implementing the GDPR into their business operations or instituting EU-style provisions into state law to continue doing business with EU residents. Bradford (2020) further notes that countries across Africa, Asia and Latin America have emulated EU data-protection standards, while US-based multinational technology companies like Apple have expanded GDPR policies to users outside the European Union.

Through these developments, the GDPR has become a de facto global privacy standard, a development that positions the European Union to become a knowledge feudalist capable of structuring the global data market to preference its economic, social and political interests. According to the United Nations Conference on Trade and Development (UNCTAD), 'Out of 120 countries outside the European Union, 67 have adopted a GDPR-like law' (UNCTAD 2021, 136). Some may view the GDPR's spread as an unqualified good, particularly for regions without data protection laws. Others, however, have critiqued this development, arguing that it may create a 'privacy universalism' that transplants a Western, specifically European, conception of privacy that results in the 'flattening of privacy values across cultures and contexts' (Arora 2019, 718). In line with traditional Western legal conceptions of privacy, the GDPR frames privacy in terms of individual choice and assumes a degree of digital literacy, which, as digital anthropologist Payal Arora (2019, 718) argues, may not be appropriate for regions that 'may perceive, experience, and value privacy in unpredictable and varied ways'.

The extraterritorial application of standards to countries that may not choose to be governed by EU-style rules and do not participate in either the making of the law or its implementation can be understood as existing within a 'neocolonial' relationship, in which 'laws and regulations . . . are not necessarily designed and executed for the protection of all citizens' (Arora 2019, 718). That the GDPR represents an imperial approach to global standard setting is sometimes not always fully appreciated by Europeans, as we learned first-hand at a pre-pandemic data and internet governance conference in Germany, to which we had been invited as presenters. During a conversation about the merits of the GDPR, a European scholar mentioned that the GDPR was designed to situate the European Union as a global privacy standard

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

setter, with those European standards intended to benefit other countries, through their adoption of these standards. We were asked what we, as Canadians, thought of the GDPR. One of us replied that we appreciated the GDPR as a thoughtful and pioneering attempt to address fundamental human rights within a commercial context. However, we said we also felt an undercurrent of resentment borne of the fact that it was designed to institute and enforce European values and rules onto other populations without us having a say, since countries and companies effectively had adopted GDPR-compliant provisions in legislation or terms-of-service agreements as the price for accessing the European market. We saw the GDPR, in other words, as a type of neocolonialism: legislation imposed upon the world without most of the world having a say in the process.

Our German hosts were, perhaps understandably, dismayed by our reaction, especially by our use of the term 'neocolonialism'. Our colleagues countered that the European Union has good intentions in designing rules intended to spread European values globally. This is undoubtedly true. However, good intentions are often in the eye of the beholder, and claiming that you have the best intentions does nothing to address fundamental issues of democratic accountability. When we asked how smaller countries might create data-governance models responsive to their specific needs and values, we were told smaller countries could choose amongst several models: a free-market US style, an authoritarian Chinese model or the EU's GDPR. Apparently, self-determination wasn't on the menu.

It would be naïve, moreover, to assume that the extension of regulatory frameworks originating in the United States, European Union or China – the three dominant digital powers – is driven purely by humanitarian concerns. As a 2021 UNCTAD report on the digital economy notes, while 'these expansion strategies towards developing countries may allegedly be grounded in international cooperation, humanitarian or development-oriented motivations, there seems to be motivation for extracting data from those countries to create value from their processing'. The UNCTAD report goes on to state:

> Thus, there is an extractive logic in these expansion strategies, which is similar to the experiences of developing countries that have specialized in natural resources production; it would result in an unequal exchange, as countries that provide raw data become highly dependent on those that extract and control them, making them flow out to foreign countries. The latter have the technological capacity to capture the value of data by converting them into digital intelligence. However, developing countries would need to pay for the imports of those data products, which could support their development, created in part on the basis of raw data originally generated domestically. (UNCTAD 2021, 112)

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

Concern about this type of imperial overreach is not limited to the world outside Europe. At the German conference, a participant from a smaller European country approached us privately to say that they agreed with our concerns, but did not feel comfortable saying so publicly.

Alongside the democratic issues with this type of transplantation of laws and norms designed for one jurisdiction (typically the Global North), countries looking to implement privacy-protection laws face other hurdles. The GDPR, after all, was developed in a relatively institutionally robust political and legal system, while other countries' situations may involve 'fragile institutions' and 'an overburdened and often weak legal system' (Arora 2019, 720). Simply passing laws and granting states greater power, in other words, will not necessarily address rights violations, especially if the actors responsible are located outside the jurisdiction in question, if the laws themselves are difficult to challenge or if national governments see greater economic or political value in facilitating, not countering, privacy-violating behaviour, such as to surveil their citizens to safeguard political stability.

The European Union is not alone in its knowledge-feudalist ambitions in setting standards to govern global flows of data. The United States, as a technological superpower and leading knowledge-feudalist state, is pursuing a similar strategy (UNCTAD 2021, 111–12). As discussed in chapter 8, the United States, Canada, South Korea, the Philippines, Singapore and Taiwan announced the creation of a Global Cross Border Privacy Rules (CBPR) System in April 2022 to govern cross-border data flows (United States Department of Commerce 2022). Both the GDPR and the CBPR approach to cross-border data flows are designed to structure the trade in data. However, as lawyer Andrei Gribakov notes, the two systems 'represent competing views on the trade-offs between privacy and economic growth', with the GDPR focused more on human rights and the CBPR rooted more in the 'desire to increase information flows and trade' (Gribakov 2019).

China, for its part, also has plans to expand its technological dominance outside the country, in part through its Belt and Road Initiative designed to enlarge the reach of the Chinese tech industry. Alongside the Belt and Road Initiative, building on efforts begun in the early 2000s, China enacted a data-protection law in 2021, the Personal Information Protection Law (PIPL) (Creemers 2022).[2] The PIPL bears a resemblance to other data-protection laws worldwide and, like the GDPR, it has extraterritorial elements, which means its provisions may apply to entities providing services to or conducting analysis of individuals on Chinese territory (Creemers 2022, 6). Like the United States and European Union, China's data policies are designed, in part, to expand its influence globally and to facilitate economic growth domestically. Paired with strategies like the Belt and Road Initiative, China's data policies may enable it to 'gain influence among third countries grappling with similar issues' (Creemers 2022, 9).

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

How the battle over data-protection standards will play out amongst the European Union, China and APEC's CBPR multilateral effort is yet to be determined (on the data-governance battle amongst China, the United States and the EU, see Carr and Llanos 2022). However, as political scientist Daniel Drezner notes, the lack of a consensus in this area amongst competing global actors reduces the likelihood of a single global regime (Drezner 2005).

ALTERNATIVE APPROACHES TO DATA GOVERNANCE

Rules setting out who can access, own and benefit from data are vitally important because, as argued throughout this book, power accrues to those who control data. How these rules are set and the resulting distribution of benefits involve questions of and negotiations over structural power, creating winners and losers. In this section we highlight collective approaches to data governance, which are attempts to deliver widely shared benefits while addressing key challenges in a knowledge-driven society, particularly pervasive surveillance and global asymmetries in the capture and control of data flows.

Collective approaches to data governance include a broad range of policies such as data cooperatives, data trusts and data sovereignty practices. These approaches vary widely in structure, purpose and degree of legal formality. Common amongst many of these approaches is a shift away from a focus on the individual to benefits accrued to or control undertaken by a collective, whether at the level of a domestic state, Indigenous nation or group of like-minded people. Benefits or control may not be shared equally or fairly amongst the population, nor are these approaches necessarily democratic in governance.

Knowledge-feudalist patterns of data extraction and commodification that disproportionately benefit a handful of Global North actors are generating a countervailing interest amongst national governments and citizens in asserting control over their data locally. The importance of understanding local contexts, conditions and populations of those providing the data aligns with the argument of Science and Technology Studies scholar Yanni Alexander Loukissas (2019, 23), who remarks that this necessitates 'forming close relationships with not only data but the conditions in which those data are manifest'. This can entail, for example, appreciating the distinctiveness of data because of its geographical, linguistic and cultural contexts. Preferences for local control over data, that is, at the national or subnational levels, can also be a political and security response for states concerned about foreign influences over technology, in what is often termed data or digital sovereignty (Musiani 2022). Such practices at the domestic level, whether in data

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

governance or policies to stimulate innovation like patent pools, are characteristic of digital economic nationalism.

Discussions about data governance tend to privilege state interests, especially when the term 'sovereignty' comes into play. However, there exist several alternative approaches to data governance, explored further next, that are premised upon the idea that data is a public good and those providing the personal data 'should have some say in what data is collected, how it is used and who benefits' (Dencik and Sanchez-Monedero 2022, 6). These include Indigenous data sovereignty, which challenges the structural power of the settler/colonial state – and, increasingly, of companies – in terms of deciding who legitimates and controls knowledge. Elsewhere, data cooperatives and trusts generally recognize that social or economic value accorded to data generally rises when data is aggregated, meaning an individual's personal data is typically not worth much on its own (Srnicek 2017), but collective actions can help people gain greater benefits than any individual could alone. Each perspective presents a different approach to how power in the knowledge structure is used, by whom and to what ends.

State Data Sovereignty and Data Localization

The role of states in regulating data has become increasingly contentious in recent years, an object of interest for democratic and authoritarian governments alike (see Haggart et al. 2021). The concept of state control of data goes by many different names – digital sovereignty, technological sovereignty, internet sovereignty or data sovereignty (see, e.g., Couture and Toupin 2019; Hummel et al. 2021). All of these terms share a general outlook, a belief central to digital economic nationalism, that states should affirm their authority over 'the Internet and the broader digital ecosystem, to protect their citizens, institutions, and businesses from the multiple challenges to their nation's self-determination in the digital sphere' (Musiani 2022, 1). Data sovereignty (we use this term for simplicity's sake) involves at its heart the issue of control: 'It depends on locally owned, controlled and operated innovation ecosystems, able to increase states' technical and economic independence and autonomy' (Musiani 2022, 2).

The concept of data sovereignty is often associated with authoritarian regimes, especially China and Russia, as both states have linked data sovereignty to broader geopolitical goals of strengthening their political standing globally (Budnitsky and Jia 2018). Both states, for example, have instituted a series of digital economic nationalist measures to extend state control over the operation of domestic and foreign technology companies within their jurisdiction, stimulate their domestic technologies industries and regulate data flows domestically (for Russia, see Stadnik 2021; for China,

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

see Jia 2021, and Luo and Lv 2021). States cannot enact such measures alone (see discussion in chapter 8), but rely upon cooperation, sometimes coercively obtained, from the private sector. Even authoritarian states face limits to their capacity for data sovereignty. Russia lacks the capacity to compel compliance from foreign tech companies in comparison to its ability to extract cooperation from its domestic industry to comply with the Russian government's efforts to regulate online content (Stadnik 2021). China, in contrast, is characterized by relatively less reliance upon foreign companies, as it has nurtured a strong domestic technology sector that the government partners with to operate its systems of online surveillance and censorship, including the Great Firewall that blocks prohibited foreign content and applications (Jia 2021).

The push towards state data sovereignty is not just coming from authoritarian countries. Policymakers around the world are increasingly focusing on 'the ability of a country to make its own decisions on data and data flows – their data sovereignty' (UNCTAD 2021, 60). Among democratic countries, the Snowden revelations about the global surveillance programmes of the US National Security Agency and its allies led many countries, including Germany and Brazil, to consider data localization policies to thwart monitoring by the US government and limit US companies' data practices (Hill 2014). Repercussions from the US knowledge-feudalist position, in this case its security ambitions, stimulated other countries' interest in digital sovereignty.

Data Localization

Data localization – the requirement that data produced or extracted from an area remain in and under the control of that jurisdiction (Sargsyan 2016) – is a key element of data sovereignty. Estonia, for example, uses data localization to protect its data sovereignty. It is often referred to as a 'digital republic' because of the country's embrace of digitization in all realms of life, including voting, taxes and the storage of all citizens' health, tax and personal records online (Heller 2017). Estonia established the first 'data embassy' in Luxembourg in 2019, a digital economic nationalist strategy intended to safeguard its data from cyberattacks, especially by Russia (Samsel 2019). Estonia's agreement with Luxembourg gives Estonia full jurisdiction over the servers holding sensitive data: Monaco is planning a similar data embassy in Luxembourg (Samsel 2019).

Sidewalk Labs' Quayside project, for its part, introduced many people in Canada to the concepts of data sovereignty and data localization. The benefits and drawbacks of the practice of data localization remain hotly debated. Opponents of data localization – and, by extension, supporters of free cross-border data flows, especially the knowledge-feudalist United States – argue

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

that data localization can reduce economic efficiency and increase the cost of doing business, while not necessarily contributing to data security (UNCTAD 2021, 50, 56). Differing regulatory frameworks across jurisdictions, for instance, can interrupt the 'global supply chain for data' by impeding 'the benefits of sharing data or making it available to researchers, developers, and innovators' (Carr and Llanos 2022, 288). Supporters of data localization, in turn, highlight that cross-border data flows tend to privilege primarily those economic powers based overwhelmingly in the Global North, particularly the United States (UNCTAD 2021, 56).

Locating data outside of the jurisdiction in which it was created can also present accountability challenges. For example, it may place data beyond the reach of domestic law enforcement. That countries have different privacy-protection standards means that data captured from the residents of one country may end up being regulated by the laws of another country, laws that they had no role in defining.[3]

During Sidewalk Labs' public consultation, key points of contention were not only how data would be governed and where it might be stored but also how the economic benefits from smart-city data might be shared amongst the local tech industry (McBride 2018). Reflecting digital economic nationalist concerns, critics questioned how governmental bodies in Canada could reclaim that data, once transferred, 'should future voters decide that this is appropriate for security or other reasons', or what would prevent the commercialization of intellectual property related to that data in ways not in the public interest once it was outside of Canada (Banks 2018).

In response to critics' concerns, Sidewalk Labs agreed to use 'its best efforts at data localization, as long as there are Canadian-based providers who offer appropriate levels of security, redundancy, and reliability' (Sidewalk Labs 2019c, 460). Sidewalk Labs' 'best efforts' may have been as much as could be obtained in the project, as some experts pointed out that mandating foreign private actors to retain their collected data in Canada could constitute a violation of the country's United States-Mexico-Canada trade agreement (USMCA). This agreement, in keeping with the knowledge-feudalist governance approach, which favours free and open cross-border data flows, bans data localization except in certain circumstances (Gribakov 2019).

The importance to the United States, the leading knowledge-feudalist state, of encouraging cross-border data flows and restricting data localization can be gleaned from comments in October 2021 by Christopher Hoff, US deputy assistant secretary for services in the US Department of Commerce. When asked what the United States' 'offensive strategy' was with respect to global privacy policy, Hoff listed three priorities: 'Tracking and combating data localization, in any form; Prioritizing direct bilateral negotiations with jurisdictions around the world; [and] Supporting the globalization and

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

expansion of the Asia Pacific Economic Cooperation Cross-Border Privacy Rules [CBPR] system' (Zweifel-Keeegan 2021; see also UNCTAD 2021, 152). On this point, it's also worth noting that the USMCA commits the three member countries not only to restricting data localization but to the APEC CBPR. This combination highlights how 'regional, bilateral and transnational trade agreements have become increasingly important instruments' not only to regulate intellectual property (see chapter 3) but also to address 'issues related to cross-border data flows' (UNCTAD 2021, 151). In both cases – data and IP – the objective is the same and reflects a knowledge-feudalist logic of maximizing cross-border exchange of commodified knowledge, with benefits accruing primarily to those actors already possessing economically valuable knowledge.

In contrast to the United States, the European Union's actions on data localization are more ambivalent and in keeping with a digital economic nationalist approach to knowledge regulation. While it formally supports free cross-border data flows, UNCTAD argues that the GDPR does not make it easy for such flows to occur, while recent privacy-related developments 'may suggest that the European Union is shifting its position on data localization' (UNCTAD 2021, 107).

Even facing such geopolitical headwinds, safeguarding data within a specific jurisdiction is not a silver bullet against abuse or domination. Depending on how data localization rules are implemented, they could restrict the ways that globally operating data companies could collect, use and store personal data from people within the jurisdiction in question. But such rules alone do not prevent problematic surveillance practices from occurring; they merely mandate that such data be housed in a specific jurisdiction. In fact, data localization policies could intensify state surveillance programmes by providing ready access to valuable caches of personal data (Sargsyan 2016).

Indigenous Data Sovereignty

In debates of data governance, states and large businesses are often perceived to be the dominant actors. The concept of Indigenous data sovereignty, however, offers a counter to governments, companies and academics, operating within an information-imperium state that seeks to appropriate and profit from data derived from Indigenous peoples, lands and cultures. There is a long, bloody history of government and industry researchers appropriating Indigenous knowledge and cultural property, and placing bodies for sale or on display in museums (Tuhiwai-Smith 1999) and disregarding cultural taboos by publicizing or profiting from cultural information, such as patenting traditional remedies for commercial gain (First Nations Information Governance Centre [FNIGC] 2016). Academics, too, have exploited Indigenous

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

knowledge for gain, often drawing inaccurate, discriminatory conclusions that have detrimentally shaped government policy towards Indigenous peoples (Walter and Carroll 2020).

Indigenous data sovereignty recognizes the fundamental point that control over the legitimation, creation, dissemination and use of knowledge is a fundamental expression of structural power. It sets out principles respecting Indigenous peoples' control over the collection, usage, storage and governance of data, placing it under the control and ownership of the Indigenous groups who created or generated the data/knowledge (Kukutai and Taylor 2016; Walter et al. 2020). Indigenous data sovereignty not only complements digital economic nationalist ideas of domestic control over data but also extends far beyond economic policies, as Indigenous data sovereignty is also a sociocultural and political response to centuries of colonialism and discriminatory state (and non-state) practices. Data sovereignty emerges from Indigenous peoples' inherent rights of self-determination and jurisdictional authority to enact laws and governance processes to create and deliver programmes, services and capacities within Indigenous communities (First Nations Information Governance Centre [FNIGC] 2016, 142). Indigenous data sovereignty movements exist in Australia, Canada, New Zealand and the United States, with efforts also underway in regions such as Southeast Asia, South America and Africa (see Walter and Carroll 2020).

Indigenous perspectives, in contrast to individualized notions of privacy and data governance, generally take a more collectivist approach to data use and control, as demographer Tahu Kukutai and population geographer John Taylor (2016) set out in their noteworthy edited volume, *Indigenous Data Sovereignty: Toward an Agenda*. Indigenous worldviews, for example, may require community or group consent for research to occur (Sherwood and Anthony 2020).

Indigenous research practices also tend to emphasize the importance of collective benefits from data collection (Sherwood and Anthony 2020). Sociologist Maggie Walter and public health researcher Stephanie Russo Carroll explain that Indigenous data sovereignty 'inverts the standard Indigenous data/policy nexus' in which the central question is not what data the state needs to deal with problems in Indigenous communities, but 'what data are needed to meet the needs, priorities and aspirations of Indigenous Peoples?' (2020, 14–15). This perspective shifts our view from a techno-solutionist framing (how can data/technology address this problem) to a more humanist framing (what problem do we want to address).

Reflecting upon collective data governance necessitates critically examining taken-for-granted ideas embedded within the digital economy, such as individualized approaches to privacy and consent. Taking collective approaches seriously entails understanding how this worldview may complement – or,

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

importantly, conflict – with other data-governance perspectives. Open data, for example, represents a popular policy solution to numerous challenges posed by a data-driven society. Open data is data that is openly accessible and usable, even for commercial purposes. The concept also includes 'government data that are usually provided for free' with 'few, if any, restrictions on reuse' (Janssen et al. 2012, cited in Scassa and Robinson 2022, 1). The push to make more government data available as open data responds to concerns that governments collect and control significant data that are beyond the reach of non-state actors. Open data proponents argue that making this data available can strengthen government transparency and accountability, while also stimulating innovation (see Robinson and Scassa 2022). Implicit in the open data perspective is a preference for free data flows (Robinson and Scassa 2022), driven by the idea – which also underlies the intellectual property regime – that the primary goal of a knowledge regime is to maximize access to and dissemination of knowledge.

An open data policy that privileges free flows of information, however, may conflict fundamentally with Indigenous data sovereignty principles, when the government data pertains to Indigenous peoples, lands and cultural knowledge. As critical data studies scholar Tracey Lauriault (2022, 25) points out, open data approaches generally overlook historical contexts and power differences amongst the entities sharing data, thereby creating tensions for Indigenous peoples who are asserting greater control over the use of their data and knowledge. In contrast to an open data perspective, decisions reflecting an Indigenous data sovereignty perspective may require restricting non-community members' access to or limiting specific cultural knowledge to insiders. Indigenous peoples in Canada, for example, are repatriating sensitive cultural objects ranging from ceremonial pipes, feathered headdresses, totem poles and pottery, to human remains from museums to their rightful Indigenous owners. Some objects are so sensitive, however, that if outsiders view them, it violates the spirit of the objects (Bernstien 2021). Contrasting questions of Indigenous data sovereignty with an open data perspective highlights a point we made in chapter 1, that the primary knowledge governance issues are related to questions of control. Considering the role and treatment of sacred art offers us a needed reminder that taking an unreflective open data perspective (or perspective on the use of intellectual property to encourage innovation or protect knowledge) involves assuming a consensus on policy objectives that may not exist between Indigenous and non-Indigenous groups or amongst countries.

Data Cooperatives

Control over data has emerged as a flashpoint in the information-imperium state, as workers struggle to assert greater control over their working

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

conditions, including collection of their data. Without access to data, gig workers know little of their working or payment conditions, how tasks are allocated or why they are disciplined or fired, while the data company controls such data for its commercial benefit. Gig workers, for example, have taken to court the ride-hailing companies Uber, Lyft and DiDi Chuxing, along with food delivery firms like Instacart, Doordash, Deliveroo and UberEats in the United States, Canada, across Europe and South Africa (Allsup et al. 2022). In these suits, workers claim that platform companies' tight control of working conditions and use of algorithmic decision-making practices means that workers are employees, not independent freelancers.

One response to gig workers' battle for access to and control over their data has been the formation of data cooperatives, similar to the long-standing cooperatives in housing and banking. Data cooperatives are groups that form around perceived collective interests in sharing and using data with individuals who want to voluntarily pool data resources (Ada Lovelace Institute 2021, 49). The Barcelona-based Salus Coop, for example, is a non-profit, citizen-driven data cooperative founded in 2017 that manages its members' health data in part by providing anonymized data for health research and for use by non-profit institutions that openly share their research results (Salus Coop n.d.).

Platform cooperatives are democratically governed and collectively owned (Scholz 2017) and, for the gig economy, are intended to provide gig workers better wages and fairer working environments (see also Woodcock and Graham 2020; Scholz and Schneider 2017). A wide variety of platform cooperatives have emerged, including Fairbnb, an accommodation alternative to Airbnb that invests proceeds in communities; Resonate, a music-streaming app owned by musicians, labels and fans; and RWASHOCCO, a Rwandan collective of coffee farmers. Driver collectives have also emerged, such as the Yatri app, which, as a taxi aggregator, represents over a thousand drivers in Kochi, India (Prabhakaran 2022).

Platform cooperatives face a difficult challenge countering gig companies' network effects as, in contrast to local cooperatives, companies like Airbnb and Uber are widely known and omnipresent in the marketplace. In contrast to the small funds of platform cooperatives, gig companies have amassed significant venture capitalist funding that enables the companies to offer artificially low prices to customers that the cooperatives cannot match, which, in turn, drives down worker pay (Scholz 2017).

Data Trusts

Similar to the concept of data cooperatives, data trusts are a type of collective data governance in which benefits from data are shared amongst people

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

who provide the personal data (Dencik and Sanchez-Monedero 2022). A data trusts, according to the London, UK-based Open Data Institute, is 'a legal structure that provides independent stewardship of data for the benefit of a group of organisations or people' (Hardinges 2018). Central to the concept of a data trust are a defined decision-making process, description of shared benefits, articulated rights and duties over stewarded data, and an independent intermediary between data collectors and those providing data, often termed 'data subjects' (Delacroix and Lawrence 2019).

Sidewalk Labs proposed a data trust to approve and oversee all data collection in the smart-city project area in Toronto (Sidewalk Labs 2019c, 383). At the time, most policymakers and the public had little familiarity with the concept. This trust, which the company envisioned as being guided by a charter, was intended to assuage public concerns over privacy and ensure data collection and use that 'spurs innovation and investment' (Sidewalk Labs 2018, 13). Problematically, argued data trust expert Sean McDonald, Sidewalk Labs was 'openly vague' about how its data trust would be structured or operate, meaning it would be challenging for anyone 'to understand the potential for credible privacy and data governance' (McDonald 2019, 2).

Depending upon how they are designed, data trusts may offer the distribution of monetary benefits, the collective power over data and independent, even public, oversight by data stewards of data access, use, storage and benefits. The London, UK-based Ada Lovelace Institute contends that the 'unique characteristic of data trusts' is that the institutional safeguards provided by trust law, at least in the context of the United Kingdom, may achieve the aim of balancing 'asymmetries between those who have less power and are more vulnerable (individuals or data subjects) and those who are in a more favoured position (organisations or data controllers)' (Ada Lovelace Institute 2021, 24). However, as Sidewalk Labs discovered, 'simply calling a data trust a "trust", or indeed any other data access architecture "trustworthy", is not sufficient', remarked Professor Dame Wendy Hall, chair of the Legal Mechanisms for Data Stewardship working group, in her foreword to the Ada Lovelace Institute report on data trusts (2021, 8).

As Sidewalk Labs learned via the Quayside project, data trusts are more complex than they first appear. Legal scholar Lisa M. Austin and computer scientist David Lie (2021, 256) observe that the concept of the data trust has been used in diverse and sometimes-conflicting ways. One set of meanings focuses on reducing technical and legal complexities regarding data protection, while the other set examines novel measures for data stewardship. As this diversity suggests, inherent within the concept of data trust are sometimes-conflicting notions of privacy and stewardship with the former emphasizing data protection and the latter focusing on managing data access:

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

two policy issues that involve separate responses that may or may not be complementary (Austin and Lie 2021).

While our focus here has been on data, the *trust* element of 'data trust' is also worth highlighting. Data trusts draw legitimacy not just from legal frameworks that purport to distribute benefits from data to the trust's beneficiaries but also from the rhetorical emphasis on 'trust'. Using the term 'data trust', observes legal scholar Christine Rinik (2020, 353), elicits a greater sense of stewardship than '"a data hoard" or "data warehouse"', even though these terms might more accurately describe a relationship involving 'the storage and exploitation of vast amounts of data by third parties'. As a result, a degree of wariness should be called for in determining whether specific data trust proposals fulfill legitimate policy objectives or are merely being deployed as rhetorical tools to elicit public trust or launder more problematic data regulation policies.

We do not discount that data trusts may have some potential to mitigate concerns over data control and ownership on different issues. However, given the challenges we outline here, policymakers need to be cautious about viewing data trusts as a simple or all-purpose tool to gain public trust. Data trusts are simply legal structures that manage data. As McDonald points out, 'data trusts manage assets, but do not inherently solve capitalism's asymmetries' or 'implicitly solve abuses of power' (McDonald 2019). Policymakers still need to think through the fundamental questions related to data governance, namely, for whom, by whom and for what purposes.

BEYOND INDIVIDUAL PRIVACY: ADOPTING A COLLECTIVE APPROACH TO RIGHTS

Contemporary privacy laws reflect a historical legal context that has generally privileged and assigned rights to individuals (Taylor et al. 2017b). Our contemporary environment, however, is characterized by several trends that challenge this individualist focus. As chapters 4 and 6 set out, there has been a dramatic increase in datasets, driven in part by the data broker industry, actors like Google and Facebook, and the rise of the consumer-oriented Internet of Things (IoT), which chapter 7 explores. Social media data, geolocational information from mobile phones, and data flowing from IoT devices provide rich detailed data. Automated tools have made it easier and more commonplace for actors to amass and parse large datasets, which combine the data of many individuals, in efforts to extract socially and commercially valuable insights, with effects that reach far beyond any one individual. These moves have led private and state actors to embrace group-level profiling, which current individual-focused privacy frameworks do not adequately address.

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

As chapter 4 cautions, actors can re-identify previously anonymized data, thereby capturing valuable personally identifiable information. But even beyond this fundamental challenge to individual privacy-focused laws, socio-legal scholar Mariana Valverde and legal scholar Alexandra Flynn (2020, 12) observe that Western privacy frameworks, focused on individual privacy, say 'very little about corporate control over the economic value of aggregate, non-personal, de-identified data' that can be used to target groups rather than individuals.

Privacy frameworks focusing on individual consent leave the public few protections in dealing with the dual problems of the data market and datafied public sector where governments employ data-fuelled analytics and automated tools to determine people's eligibility for services like welfare or housing. These decisions are made by identifying individuals as part of a group, not as individuals themselves. Ordinary people are caught in the rapidly evolving data economy and are expected to be capable managers of their personal data, even though research demonstrates that people cannot manage all the ways that companies use, and often abuse, their personal data (Obar 2015). In contrast to some private-sector data collection, people generally cannot opt out of interacting with their governments.

Any policy response aimed at addressing the deep-seated and structural problems we've discussed as inherent to the rise of the information-imperium state must go beyond individualistic notions of privacy and informed consent. Such an approach does not require ignoring or minimizing individual privacy rights: these are fundamental human rights and should be treated as such. Rather, the concepts of data justice and group privacy should be important complements of individual-based privacy. Both concepts adopt human rights-driven, collective approaches to governing data that fundamentally challenge the dataism and pervasive state/corporate surveillance integral to the information-imperium state.

Data Justice

Approaching data within a collective rights framework requires a consideration of the ways in which data-driven practices undertaken by states and private actors create harm. The concept of data justice is an alternative to individualistic approaches to human rights, as the concept takes a social justice-driven approach to resisting the modern datafied society (Dencik et al. 2016; Taylor 2017b). Communication scholars Lina Dencik et al. (2019, 181) have developed data justice as a concept that foregrounds questions about power relations in the collection, use and commodification of data, including how we may consider ideas of security, equity, fairness and sustainability in a data-driven society in which some groups reap enormous benefits and others are excluded.

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

A data justice approach is intended to transform concerns about privacy, data protection and surveillance from specialized 'digital' issues into 'a core dimension of social, political, cultural, ecological and economic justice' (Dencik et al. 2019, 181). In other words, questions about privacy, consent and governing data are not technical but rather fundamental to our society. Data justice does not focus merely on strengthening existing rights like privacy. Rather, it should be understood as 'a system-level critique' that does not focus on a specific type of data collection or technology 'but rather how datafication features in on-going negotiations of social relations and power dynamics within society' (Dencik and Sanchez-Monedero 2022, 8). In short, data justice aims to challenge and resist the 'central position of data in contemporary capitalism' (Dencik et al. 2019, 181).

As it is a concept intended to achieve social justice goals, data justice has concrete aims. Law and technology scholar Linnet Taylor (2017b) sets out these aims in three pillars: (in)visibility, anti-discrimination and (dis)engagement. The first pillar recognizes that sometimes people are too visible, as states or companies subject them to intense, often discriminatory, surveillance or profiling, especially if they are poor or otherwise marginalized, while other times people are overlooked or undercounted, leaving people without access to services. Addressing these two extremes entails recognizing that it is important people are represented accurately and appropriately (visibility), and are treated fairly and equitably (invisibility). Second, people should have a right to non-discrimination to identify and challenge bias in data use (Taylor 2017b, 9).

Finally, the pillar of (dis)engagement requires that people have the freedom to control the terms of how, or even if, they engage with data markets, including determining how their data is used and by whom (Taylor 2017b, 9). In practical terms, this means that people should be able to decide to opt out of specific private-sector data collection activities. This essentially involves a wholesale withdrawal from the datafied society and economy which operates according to the imperative that if information can be collected, it must be. The freedom to disengage from commercial databases has not yet been adequately theorized, as even privacy scholars generally 'assume that such engagement is inevitable' (Taylor 2017b, 10).

Adopting a data justice approach requires considering seriously how and where state and corporate data practices should be limited to address related harms like that of discrimination, as well as exploring the potential consequences of such limitations. A core element must also involve considering the nature and implications of data decommodification by examining how people may opt out of data markets, thereby removing their data from private actors or somehow remaining off-limits from data collection.

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

Group Privacy

The concept of group privacy is a response to private-sector and state uses of automated data tools to process massive amounts of data, often with a focus on group-level analysis. As scholars studying privacy point out, 'the individual is often incidental to the analysis. Instead, data analytical technologies are directed at the group level' (Taylor et al. 2017b, 2). This expansion of analytical focus from the individual, where privacy frameworks apply, to groups, where privacy frameworks are absent, 'challenges the very foundations of most currently existing legal, ethical and social practices and theories' (Taylor 2017b, 5). Simply put, as we note in chapter 4, we are in a situation where contemporary legal frameworks do not adequately address group-level data effects.

As we saw in chapter 6, fears of privacy violations or exposure to discrimination from group-level analysis are not abstract concerns. Genetic data, for example, complicates the notion of individual privacy as it reveals information not only about a specific individual but also their immediate and extended family members without their consent (Hallinan and de Hert 2017). The use of genetic data has received media attention as law enforcement has begun using consumer-oriented ancestry DNA databanks like GEDmatch to solve cold cases where genetic material (e.g., via a suspect's blood sample) was recovered (e.g., Chamary 2020). While catching violent offenders is laudable, law enforcement's use of consumer-oriented DNA companies raises critical questions of privacy and consent, as DNA samples uploaded for one consented purpose (ancestry research) can be (and are being) used to detect suspects and, in doing so, reveal genetic connections between individuals without their consent. In other contexts, law enforcement generally must obtain a legal order to access an individual's genetic material, raising concerns that police may use commercial DNA databanks indiscriminately.

The notion of group privacy or collective privacy has promising utility to address this gap in data protection. Group privacy has gained prominence in recent years, most notably in the edited volume *Group Privacy: New Challenges of Data Technologies* (Taylor et al. 2017a; see also Loi and Christen 2020; Puri 2021; Arora 2019). Philosopher and legal scholar Edward J. Bloustein (1978; see also 2017) was one of the first to articulate the concept of group privacy, but the idea is also evident in scholarship on privacy, to varying degrees, as 'relational privacy' or 'family privacy' (e.g., Westin 1967; see also Floridi 2014).

Definitions of group privacy vary broadly, as scholars from different disciplines explore what this new approach to privacy might entail (e.g., Loi and Christen 2020; Puri 2021). Legal scholar Alessandro Mantelero provides a useful starting point in describing collective privacy as 'the

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

right to limit the potential harms to the group itself that can derive from invasive and discriminatory data processing', particularly 'the unfair and harmful use of data that is processed using modern analytics' (Mantelero 2017, 148).

Group privacy, as understood by Mantelero and others, is not intended to replace individual privacy rights but rather to act as an 'important complement to individual privacy' (Taylor et al. 2017, 236). Individual privacy rights would continue to have legal protections attached, for example, to the collection and use of personal information, but group privacy would form a yet-to-be-determined additional layer of protection. A key part of group or collective privacy is deciding how to identify the cluster of individuals forming the grouping. This point may seem merely philosophical – at what point do individuals constitute a group? – but there are practical implications to this discussion. For the concept of group privacy to have meaning, the group itself needs to be somehow defined, as when 'some threshold of unity or identity has to be reached' (Jones 2016; cited in Loi and Christen 2020, 217).

Defining what constitutes a group is challenging. Do members self-define or can they be unaware that they belong to a particular group? Groups can be dynamic in their formation and membership. If the criteria constituting the group change, such as from people genetically prone to one disease to another health condition, then the group will change. Reasons for the creation of algorithmically generated groups, discussed in chapter 6, may only be known to the algorithm and its designers (Kammourieh et al. 2017; see also Loi and Christen 2020). Even if people were aware that group profiling affected them, when the origin and nature of such data practices are not publicly disclosed, there are few options available to challenge the conclusions.

Group privacy usefully provides the beginnings of a new vocabulary to counter some of the negative consequences of the information-imperium state and its overly commercial approach to data regulation. Of course, identifying and protecting group privacy rights does not automatically address the structural problems of mass data extraction and commercialization inherent to the data economy. Consequently, we argue that combining data justice and group privacy offers a useful perspective. Both data justice and group privacy reject the notion – foundational to the data economy – that people are individual rational consumers who should be responsible for managing companies' collection and use of their personal data (e.g., Taylor et al. 2017). Relatedly, both concepts push back against a mode of capitalism that views the datafication of all manner of social activities and personal attributes as somehow 'natural' or uncontested (e.g., Dencik et al. 2019). Instead of viewing people as consumers voluntarily and knowledgeably negotiating their way through a datafied society and economy, both concepts emphasize people's identity as 'citizens requiring data protection' (Taylor et al. 2017, 234). Government restrictions

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

on the type of personal data that private actors can collect and monetize are important elements of the broader process of data decommodification.

CONCLUSION

There are important geo-economic and geopolitical ramifications to data-governance debates, as states jockey for primacy in the control of the knowledge structure. Rules governing knowledge (in the form of data and intellectual property) are highly contested, as the regulatory and trade battles amongst the United States, European Union and China illustrate. These great powers are each forging ahead with their own plans for the data economy, with the latter two aspiring to become knowledge-feudalist states to counter the United States. Smaller states, in contrast, must determine how best to meet their domestic needs, which may include aligning with one of the great powers or enacting digital economic nationalist policies as a bulwark to protect domestic interests. Conflicts over how data should be conceptualized and governed exist not only among states but also between (and within) states and Indigenous nations. Recognizing the legitimacy of Indigenous data sovereignty requires taking seriously Indigenous group's rules prohibiting the sharing or commodification of sensitive knowledge (Kukutai and Taylor 2016; Walter et al. 2020). In some cases, Indigenous data sovereignty may conflict with governmental or civil-society preferences for open data, especially in relation to knowledge Indigenous groups deem sensitive or culturally important. This is because the fundamental issue regarding data – and knowledge governance – is around the question of control and who should decide the ends that should be pursued in regulating knowledge.

Shifting from an information-imperium state view premised upon the all-encompassing control of knowledge to a collective rights approach will be challenging and involves countering powerful state and industry interests that have accumulated considerable authority in a datafied society and economy. A central element of effectively countering negative knowledge-feudalist measures is a strong democratically accountable state, one that is bolstered and pushed forward by an engaged civil society. However, the degree to which governments have the necessary skills, resources and desire to regulate the digital economy and institute effective protections for human rights is an open question. Capacity will vary amongst countries but state action should be responsive to local contexts and needs rather than being driven by transnational business interests. Public regulators and governmental officials will require expertise in digital policymaking, intellectual property and data governance, amongst other key issues.

The New Knowledge by Blayne Haggart & Natasha Tusikov / Open Access PDF from Rowman & Littlefield Publishers

Adopting a human rights-driven collective rights approach also requires a fundamental shift in mindset. Instead of viewing people as consumers voluntarily engaging in the trade of personal data, people must be understood as citizens (broadly interpreted) who deserve to have their rights protected. Such a shift necessitates direct state action to ensure that data activities are 'linked to citizenship and accountability' (Taylor et al. 2017, 234). Data justice and group privacy provide a vocabulary and set of policies, situated within the larger approach of data decommodification, that potentially offer tangible data-protection benefits, such as enabling people to opt out of data markets. As they are relatively new, further work is needed by academics, civil-society groups and policymakers to develop and operationalize these concepts. An important element of this research will be to consider how they might be adapted to different sociocultural and political contexts to meet local needs.

NOTES

1. For a detailed examination of the GDPR, see Edwards (2018).
2. Unlike the GDPR, China's PIPL does not recognize privacy as a fundamental right, nor does it impose restraints on government bodies to collect and process data, although it does set out the data collecting powers and limitations of individual government departments (Creemers 2022, 8).
3. This point is often used to argue that data collected in one country may be subject to privacy-invading laws in the data-extracting country, as with the USA PATRIOT Act's expansive rules for government surveillance. The more fundamental point is that countries may have legitimate differences on what privacy legislation should look like. What this means is that the fundamental critique of cross-border data flows is linked to the lack of democratic accountability, not necessarily the nature of the privacy regime.