CHAPTER 6

Data policies, laws, and regulations: Creating a trust environment

Main messages

1. Trust in data transactions is sustained by a robust legal and regulatory framework encompassing both *safeguards,* which prevent the misuse of data, and *enablers,* which facilitate access to and reuse of data.

2. Safeguards must differentiate between *personal data,* requiring a rights-based approach with individual protection, and *nonpersonal data,* allowing a balancing of interests in data reuse.

3. Enablers for data sharing are typically more developed for *public intent data,* where public policy and law mandating data access and sharing are more readily established, than for *private intent data,* where governments have more limited influence.

4. Creation of a trust environment remains a work in progress worldwide, especially in low-income countries. There is no one-size-fits-all legal and regulatory framework. In countries with weak regulatory environments, the design of suitable safeguards and enablers may have to be carefully adapted to local priorities and capacities.

A trust framework of data safeguards and enablers

With the growing recognition of the use, misuse, and underuse of data, responsible governance of data has gained importance, resulting in new global legal and regulatory standards. This movement was propelled by the revelations in 2013 by US whistleblower Edward Snowden of global surveillance by Western democracies,[1] followed by the Cambridge Analytica scandal in 2018.[2] In response, countries enacted major policies to protect data. A series of epochal rulings by India's Supreme Court identified a constitutional right to privacy, and the country is now considering new data protection legislation. In the European Union (EU), its General Data Protection Regulation (GDPR) came into force in 2018 with its application beyond the EU's borders,[3] and it inspired similar legislation in other jurisdictions, such as the US state of California.[4] China implemented its Personal Information Standard in 2018, promulgated its Civil Code in 2020, and introduced a new draft Personal Data Protection Law for public consultation in 2020.[5] Despite these important advances regarding personal data, legal frameworks for data governance across much of the developing world remain a patchwork, raising concerns about the ability of lower-income countries to benefit from the development opportunities emerging from the burgeoning global data economy.

This greater attention to the use and reuse of personal data is part of an evolving social contract around data, which remains under negotiation across the globe (see spotlight 6.1 for an example of how COVID-19 is creating new challenges for using data while protecting rights). With a view toward informing this process, this chapter lays out the legal mechanisms that enable trusted and trustworthy domestic and cross-border data transactions for the use and reuse of both personal and nonpersonal data. Whether the focus is on the collection, use, transfer, or processing of data between businesses, or among citizens, businesses, and governments, each of these interactions is a data transaction with the potential to create value—as long as both parties trust the overall process sufficiently. However, a variety of factors can undermine trust. These may include the absence, weakness, or uneven application of the legal framework; weak institutions and law enforcement or lack of effective ways for parties to enforce their rights; practices that unfairly benefit certain actors; skewed or lopsided incentives (see chapter 8); and poor or insecure infrastructure (see chapter 5).

From a normative perspective, trust is a function of both "hard law" and "soft law." *Hard law* includes domestic, regional, and international law, as well as case law and statutory law that originate from tort, contract, and competition law. Some of the issues embedded in domestic law have their origins in well-hewn and commonly agreed standards derived from international law, conventions, and treaties. Emerging applications of trust law and competition law may also play a valuable role in strengthening the normative framework for data.

Whereas *hard law* is shaped by state actors, *soft law* includes standards, terms and conditions of use, norms, and codes of conduct and other voluntary frameworks used by nonstate actors, including industry participants and civil society (see chapter 8). These soft law elements can play an equally valuable role in governing data use according to needs and cultural specificity.[6]

A central claim of this Report is that use of data for development purposes requires a legal framework for data governance that includes both safeguards and enablers. *Safeguards* generally refers to those norms and legal frameworks that ensure and promote trust in the data governance and data management ecosystem by avoiding and limiting harm arising from the misuse of data or breaches affecting their security and integrity. *Enablers* generally refers to those policies, laws, regulations, and standards that facilitate the use, reuse, and sharing of data within and between stakeholder groups through openness, interoperability, and portability. Whereas the approach to safeguards differs markedly for personal and nonpersonal data, a common set of enablers is relevant to both categories.

For the collection and processing of *personal data*, this Report proposes a rights-based approach, whereby access to personal data must first be adequately safeguarded before enabling use and reuse. This two-step process helps to rebalance power asymmetries between data holders/subjects and data controllers/users that can undermine trust. For the purposes of this chapter, personal data include not only data directly provided by an individual, but also personally identifiable information and machine-generated information that can readily be linked to an individual (such as mobile phone data).[7]

For *nonpersonal data*, this Report advocates a balance of interests approach to safeguards and enablers, recognizing that trade-offs typically arise between increasing data access and safeguarding intellectual property rights (IPRs) over nonpersonal data. The focus is thus on a legal framework that

enables the (re)use and sharing of data through regulatory predictability, data openness, and portability (the ability to readily transfer data from one service to another based on clear legal and technical standards). Of growing importance are data that blend both personal and nonpersonal sources—so-called mixed data.

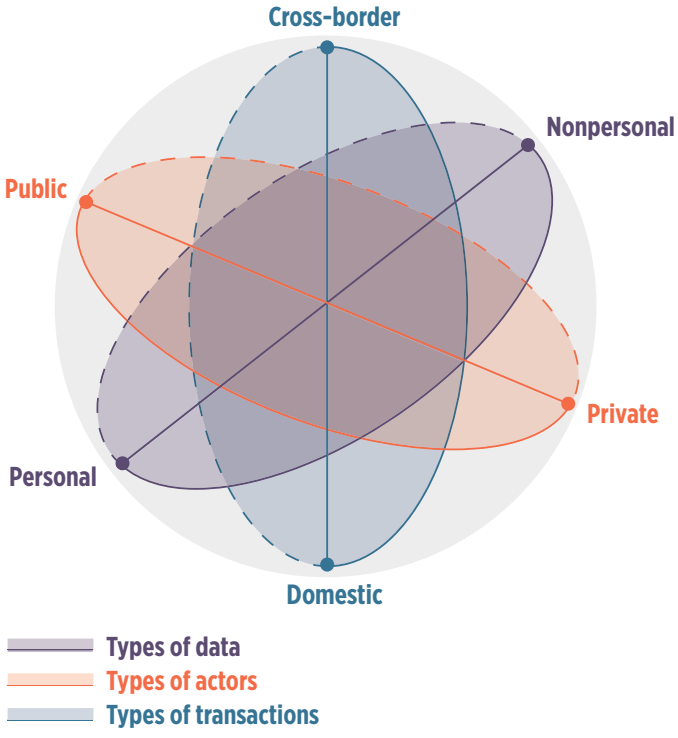
The creation, collection, and use or processing of personal and nonpersonal data by public or private sector entities in both domestic and cross-border contexts interact in a dynamic way in a three-dimensional legal/regulatory space in which different elements of the legal framework apply (see figure 6.1). The underlying type of data does not necessarily determine how the data might be treated legally across the data value chain; that depends on how such data are used or processed. For example, data that may start off as public sector and personal data (such as household survey, health, or geolocation data) may end up as private sector and nonpersonal data (when integrated as part of a proprietary algorithm and perfectly deidentified). Similarly, data that start out as private data may end up in the public domain if published as open data or shared with government under a data sharing agreement. These dynamic shifts in data uses may change the legal treatment of that data accordingly.

The trust framework encompassing safeguards and enablers is underpinned by rule of law and good governance principles. These include certainty, transparency, accountability, nondiscrimination, fairness, inclusiveness, and openness. They are subject to due process limitations such as necessity and proportionality. Transparency, accountability, and certainty in rulemaking can be reinforced by ensuring that laws and regulations are developed according to good regulatory practices. These include supporting consultative rulemaking[8] and ensuring that regulations are based on evidence, with stakeholder impacts and spillover effects fully considered through regulatory impact analysis.[9] In addition, recent developments in regulatory design have included efforts to adapt regulations to the digital age. Mechanisms such as regulatory sandboxes and laboratories help make regulations more agile and readily adaptable to evolving circumstances. By drafting principle-based and technologically neutral laws and regulations, policy makers help them remain relevant as technologies evolve and reduce compliance burdens.

To capture the current robustness and completeness of normative frameworks for data governance around the world, the chapter draws on a new Global Data Regulation Survey conducted exclusively for this Report.[10] It collected information on attributes of the regulatory framework in 80 countries (covering 80 percent of the world's population) selected from global regions and country income groups across the development spectrum. The survey entails a detailed assessment of domestic laws, regulations, and administrative requirements, reflecting the regulatory status of each country as of June 1, 2020. Survey results are summarized in a variety of subindexes that capture different aspects of the regulatory environment for safeguards and enablers.

This chapter focuses squarely on the legal dimension of data governance. Chapter 7 then examines the resulting economic trade-offs, and chapters 8 and 9 discuss the design of institutional ecosystems to support implementation and enforcement.

Figure 6.1 Envisioning the multidimensional nature of the legal framework for trust



Source: WDR 2021 team.

Building safeguards for trusted data use

The term *safeguards* refers to the trust environment around the collection and use of data. It includes supporting individuals' agency—that is, their ability to exercise control—over how their personal data are used, through mechanisms such as consent, rights

of use of data, and regimes that allow reuse of data for "legitimate purposes" without express consent. Safeguards also encompass how data are secured and accessed, covering the obligations of those who collect, process, or use data to take precautions to ensure the integrity of the data and protect data rights, including intellectual property rights and other limitations on the use of nonpersonal data (see figure 6.1).

Safeguards are analyzed primarily according to whether they are related to personal data, nonpersonal data, or mixed data. The degree of sensitivity of these types of data differs markedly, leading to various legal approaches.

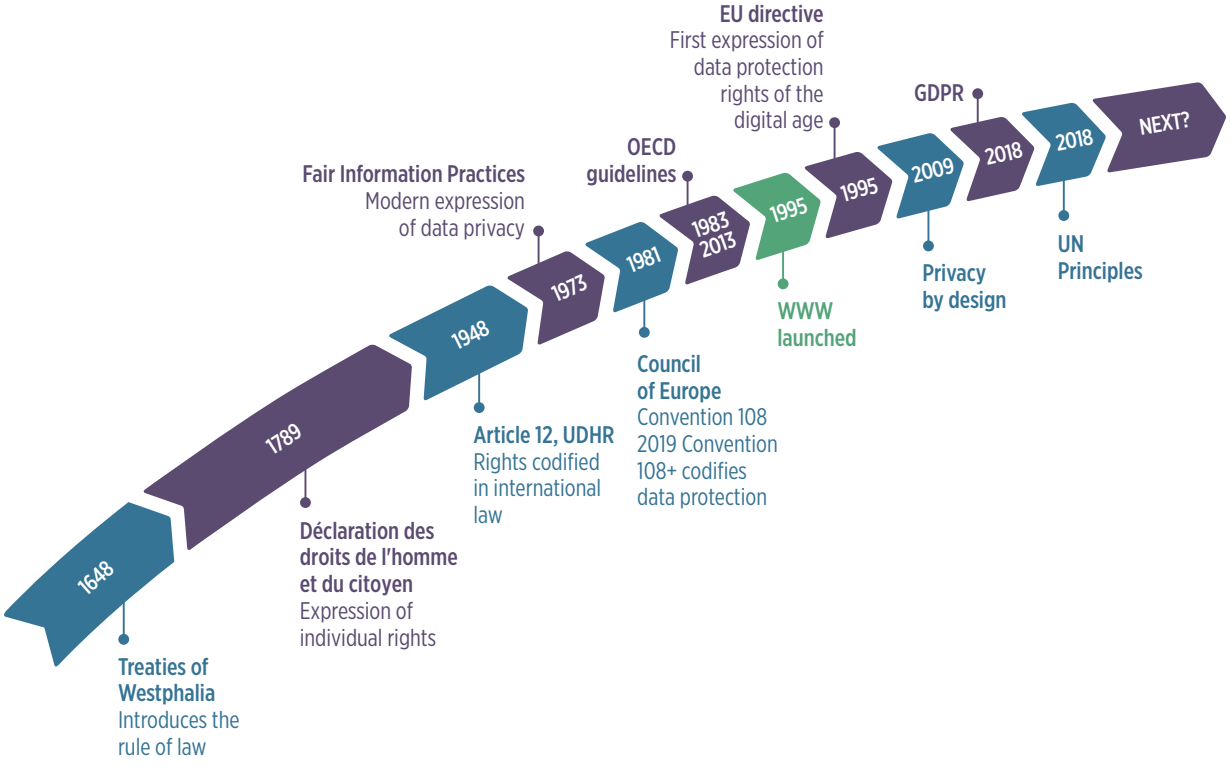
Safeguards for personal data, nonpersonal data, and mixed data

Safeguards for personal data are grounded in a rights-based framework that has evolved over time (see figure 6.2). These safeguards have their origin in the establishment of the "rule of law" in conjunction with the expression of individual rights in the Enlightenment and were codified in international law after World War II. They were further refined in the context of analog data in the 1970s and 1980s with the Fair Information Practices, the Council of Europe's Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data,[11] and the first guidelines issued by the Organisation for Economic Co-operation and Development (OECD). Safeguards must necessarily adapt to technological change and will continue to evolve accordingly. For example, the OECD guidelines were updated after the launch in 1995 of the World Wide Web, and Convention 108 was updated to Convention 108+ in response to the entry into force of the GDPR.

Safeguards for nonpersonal data entail a more straightforward balancing of economic incentives and interests, grounded in IPRs as typically enshrined in domestic law.

For datasets containing mixed data, it is the responsibility of the data processing entity to ensure that personal data are protected. This compliance challenge has become more acute in recent years because source data and collection methods have evolved and

Figure 6.2 The evolution of data protection



Source: WDR 2021 team.

Note: This figure shows a clear arc from historical concepts of rights governing interactions between the state and the individual (and between states) to principles guiding data protection. EU = European Union; GDPR = General Data Protection Regulation; OECD = Organisation for Economic Co-operation and Development; UDHR = Universal Declaration of Human Rights; UN = United Nations; WWW = World Wide Web.

blurred the distinction between the traditional legal definitions of personal and nonpersonal data.

The Global Data Regulation Survey conducted for this Report provides an overview of the extent to which good-practice data safeguards have been adopted. Across the 80 countries surveyed, about 40 percent of the elements of good-practice regulatory safeguards are in place. Although scores range considerably, from less than 35 percent in low-income countries to more than 50 percent in high-income countries, the results highlight that even among the latter the regulatory framework is far from complete. Of the high-income countries included in the survey, Australia, the United Kingdom, and Uruguay stand out as those with the most advanced safeguards. Among the strongest middle-income countries are Colombia, Moldova, and Nigeria. Other low- and middle-income nations that have endeavored to develop safeguard regulatory frameworks are Benin, Mexico, and Turkey. Mauritius, a standout among its middle-income peers, performs well on most safeguard measures. It has deliberately designed and implemented policies based on best practices and has distinguished itself as one of the first Sub-Saharan African countries to ratify Convention 108+. In Latin America, Uruguay is one of two countries to have received an adequacy determination from the European Commission.

Overarching safeguards for cybersecurity and cybercrime

A key element in establishing trust in the data ecosystem for both personal and nonpersonal data is ensuring the security of the network infrastructure and elements over which data flow.

Cybercrime laws effectively give teeth to cybersecurity policies. Although there is no universally accepted definition of cybercrime, the concept encompasses both a narrow view—criminal activities targeting information and communication technologies (ICT) and software—and a broader view—traditional crimes committed in cyberspace.[12] In practice, the scope of cybercrime is typically understood to include unauthorized access to a computer system (sometimes called hacking), unauthorized monitoring, data alteration or deletion, system interference, theft of computer content, misuse of devices, and offenses related to computer content and function.[13]

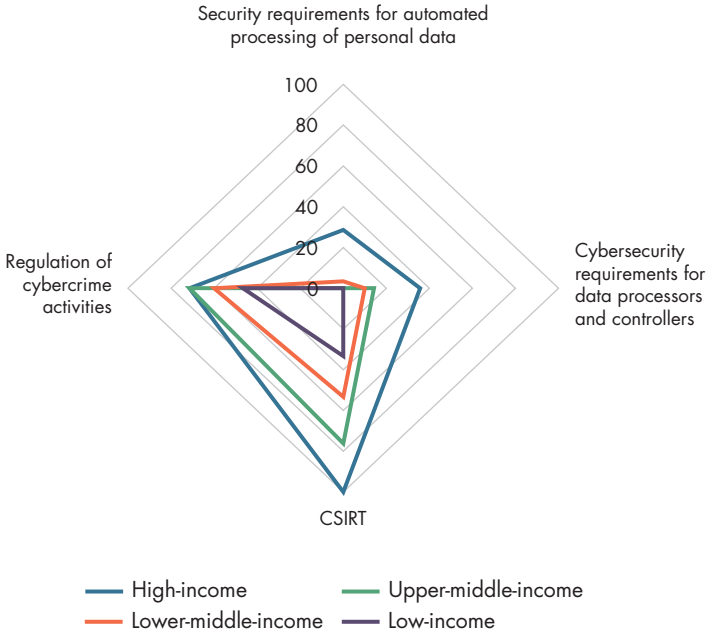
Cybercrime knows no borders. The crime can be committed from any computer, no matter where, connected to the internet or from a public or private entity that relies on ICT systems. Similarly, the impact of the crime can be felt anywhere, even outside the jurisdiction where the cybercriminal is physically located. Thus to be truly effective, a cybercrime law needs to extend beyond dealing with criminal activity within a subnational or national jurisdiction and become a tool to maximize cross-border cooperation.[14] This requirement entails the legal notion of dual criminality, which establishes that a criminal activity in one jurisdiction is also a criminal activity in another.[15] It also demands practical collaboration, usually achieved through mutual legal assistance treaties (MLATs).

Countries enter into MLATs either through bilateral treaties with other countries or by adhering to an instrument that features a built-in MLAT process, such as the Council of Europe's Budapest Convention of 2001. The main legal instrument for cybersecurity in Europe and beyond, this convention provides for balancing security interests with respect for human rights.[16] Sixty-five countries have acceded to the convention, with an additional 12 states participating as observers.[17] Of the members and observers, 26 countries are lower-middle-income. Recently, some governments have been sidestepping the MLAT process by making requests for evidence directly to foreign law enforcement agencies and allowing them to do likewise. In this vein, the United States adopted the Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018, which authorizes the US government to enter into bilateral agreements with foreign governments, allowing the parties to remove any legal barriers that would prevent the other party from seeking and obtaining data directly from the service providers in the other country under certain circumstances.[18] This has attracted comment for potentially sidestepping legal protections for personal data.[19] The European Union is considering a draft regulation with similar provisions.[20]

Cybersecurity encompasses the data protection requirements for the technical systems used by data processors and controllers, as well as the establishment of a national Computer Security Incident Response Team (CSIRT), an expert group that handles computer security incidents (see chapter 8). In addition to dealing with the criminal behaviors discussed, cybersecurity also builds trust by addressing unintentional data breaches and disclosures (such as those resulting from badly configured servers) and holding firms accountable.

Overall, the Global Data Regulation Survey reveals a low level of uptake of cybersecurity measures (figure 6.3). None of the low-income countries included in the survey has legally imposed a full range of security measures on data processors and controllers. Even among high-income countries, barely 40 percent

Figure 6.3 Gaps in the regulatory framework for cybersecurity are glaring across country income groups



Source: WDR 2021 team, based on World Bank, Global Data Regulation Survey, https://microdata.worldbank.org/index.php/catalog/3866. Data at http://bit.do/WDR2021-Fig-6_3.

Note: The figure shows the percentage of countries in each country income group that had adopted good-practice legal and regulatory frameworks for cybersecurity and cybercrime as of 2020. CSIRT = Computer Security Incident Response Team.

of those surveyed require data processors and controllers to comply with these security requirements, such as by adopting an internal policy establishing procedures for preventing and detecting violations; establishing the confidentiality of data and systems that use or generate personal data; appointing a personal data processing or information security officer or manager; performing internal controls; assessing the harm that might arise from a data breach; or introducing an awareness program among employees. CSIRTs are far more prevalent. They can be found in all high-income countries and in about one-third of low-income countries.

Among the lower-middle-income group, a good reflection of best practice is the comprehensive cybersecurity requirements in Kenya's new Data Protection Act. It requires data controllers to consider measures such as pseudonymization and encryption of data; an ability to restore the availability of and access to personal data in the event of a physical or technical incident; and mechanisms to identify internal and external risks to personal data that are reasonably foreseeable. It also requires steps to ensure that safeguards are established, effectively implemented, and continually updated in response to new risks or deficiencies.

Safeguarding personal data

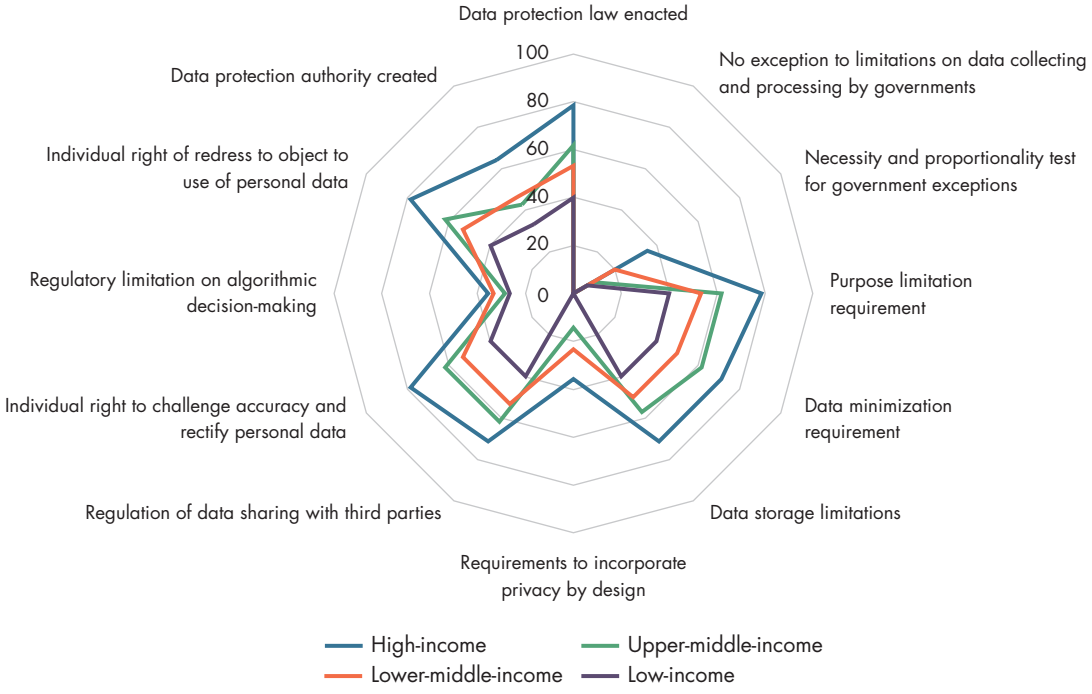
To better address underlying concerns about the power asymmetries between (individual) data subjects and data processors and collectors, this Report advocates an approach based on control over personal data rather than one grounded in data ownership (see spotlight 6.2). Under the rights-based approach to protection of personal data, individuals have fundamental rights regarding their personal data. These rights are both substantive and procedural.

Substantive rights include measures preventing the unauthorized disclosure of personal data and the use of personal data for unwarranted surveillance, unfair targeting, exclusion, discrimination, unjust treatment, or persecution. Such substantive rights also require purpose specification, data minimization, and storage limitations.

Procedural rights are built around the concepts of necessity, transparency,[21] accountability, proportionality, and due process. They include rights to receive notice about and to object to how data are used and rights of access to correct and erase data (including the right to be forgotten),[22] as well as rights to redress and remedy. These rights are grounded mainly in domestic law. The absence of a harmonized global legal framework for protection of personal data affects cross-border data transactions involving personal data, which are especially limited in lower-middle-income countries (see chapter 7).

Adoption of data protection laws is comparatively widespread.[23] Nearly 60 percent of countries surveyed for this Report have adopted such laws, ranging from 40 percent of low-income countries to almost 80 percent of high-income countries (figure 6.4). Yet the quality of such legislation is uneven, with important good-practice elements often lacking. Legal frameworks for the protection of personal data should typically include individual rights to challenge the accuracy and object to the use of personal data and parallel requirements for data processors to limit the purpose of data use, minimize the volume of data collected, and limit the time frame for data storage. These legal provisions are much less prevalent in low- and middle-income countries than in high-income countries. Although many lower-middle-income countries have laws on the books, their enforcement is uneven: only some 40 percent of low-income and lower-middle-income countries have created a data protection authority, compared with some 60 percent of high-income countries.

Figure 6.4 Progress on personal data protection legislation differs markedly across country income groups



Source: WDR 2021 team, based on World Bank, Global Data Regulation Survey, https://microdata.worldbank.org/index.php/catalog/3866. Data at http://bit.do/WDR2021-Fig-6_4.

Note: The figure shows the percentage of countries in each country income group that had adopted good-practice legal and regulatory frameworks to safeguard personal data as of 2020.

The uneven quality of data protection legislation affects in practice the effectiveness of safeguards for personal data.

After many years in the making, both Kenya and Nigeria recently updated their legal regimes for data protection. In 2019 Kenya's new Data Protection Act entered into force, while Nigeria's National Information Technology Development Agency issued a new Data Protection Regulation. Both instruments reflect many of the elements contained in the GDPR. India is also debating landmark data protection legislation.

Requiring consent or other lawful bases for data collection and processing. Most data protection laws rely on individual consent as one lawful means of limiting how data about individuals can be collected and used.[24] The appropriate lawful basis for data processing depends on factors that include how the data will be used and the relationship between the parties. For example, consent may not be the appropriate basis for data processing by public authorities.[25]

The consent model has normative and practical limitations. Current commercial practices often adopt a "tick the box" approach to obtaining consent, and they are more often based on incentives to limit corporate liability than on a desire to ensure that consent is "informed" (that is, that individuals fully understand what will happen to the information they have authorized for collection and are effectively in control of how their data will be further used and shared). Privacy notices are often long, complex documents written by companies' legal teams. It is, then, difficult for people to read all the disclosure documents on the websites they visit or for all the apps on their smartphones.

This difficulty is particularly acute in the developing world, where literacy rates remain low and individuals face language and technical barriers to understanding privacy notices. In such cases, data processors should take extra care to obtain informed consent through adapted means. Firms can use consent to justify collecting and processing excessive amounts of data, especially in countries where data protection authorities may not have enough resources to monitor and enforce compliance with other obligations, such as data minimization. Addressing these concerns would require taking a more user-centric approach to obtaining informed consent for the collection of volunteered data, including using

simplified terms of service and embedding responsible data collection practices in operations to avoid collecting excessive amounts of data.

Although consent may still be an appropriate lawful basis in some instances (such as when data are volunteered by individuals), newer technologies involving passive data collection (such as by the Internet of Things) and merging or linking datasets to make inferences pose further challenges to the consent model.

Alternatives to consent include relying on other lawful bases for processing personal data, including resorting to a "legitimate purpose" test or fiduciary duty requirement. A legitimate purpose test would limit the use of personal data to what is compatible, consistent, and beneficial to data subjects based on the original purpose for which the data were collected. Under this approach, data could still be used for more wide-ranging purposes if they are anonymized or aggregated to, for example, develop new products and services, or to make risk assessments without impinging on the data subject's rights. Relying on a fiduciary duty approach would require data collection and processing firms to always act in the best interests of data subjects and in ways that are not detrimental to them. Legally obligating providers to act in the best interests of their customers can help establish trust and confidence among customers that their data are being used responsibly. Examples of fiduciary duty breaches include using customer data to unfairly manipulate purchasing decisions. Another alternative to these approaches that might require less oversight is to ban use of certain types of data outright based on identified possible misuses of personal data.[26]

In principle, the limitations on the use of personal data enshrined in data protection legislation apply to all parties that process or control personal data. Nevertheless, governments may choose to create exceptions to these compliance and liability limitations for data processing by public sector entities. The Global Data Regulation Survey indicates that these exceptions are widespread in all surveyed countries that have data protection legislation (figure 6.4). Most of these exceptions are limited and pertain to specific data uses, such as in relation to national security as in Brazil and India[27] or in transactions involving health data as in Gabon. Other countries have passed laws that provide for more wide-ranging exceptions, including exemption from the requirement to obtain consent from data holders when performing lawful government functions such as service delivery.[28]

Where such government exceptions exist, good practice calls for them to be transparent and objective. They should also be limited in scope and duration (such as through sunset provisions) to respect due process limitations. These exceptions must be "necessary and proportionate" to the intended objectives—limitations designed to ensure that any established exceptions are lawful and balanced against the objective being sought.[29] Furthermore, exceptions should be consistent with international human rights law. More than one-third of high-income countries require justification for the exceptions, while less than 10 percent of surveyed low-income countries place such process limitations on government action. This lack of limitations creates additional opportunities for unchecked state surveillance or mission creep, thereby undermining trust in data use.[30]

Meeting technological challenges. Rapid technological progress in data processing, machine learning, and artificial intelligence (AI) pose challenges to current data protection frameworks. In particular, traditional data protection is based on the notion that information is volunteered by the data subject, whereas data analysis is increasingly based on observed data (obtained from passive scraping of information from devices and social media accounts) or inferred data[31] (generated from a vast array of correlates using statistical techniques). In addition, AI and machine learning rely on large-scale datasets to function, creating tensions with established data protection principles such as data minimization. Although linking these data sources provides a fuller picture of the individual, the linked data could also have a negative impact on the subject if used in decisions such as on credit or employment, with limited enforceability of the protections applicable to volunteered data, including accessing and seeking correction of erroneous information.

The increasingly widespread practice of linking datasets to feed algorithms also stretches the limits of technical mechanisms to protect personal data, such as anonymization. Unlike pseudonymized data, once data are thoroughly deidentified legally they are no longer considered to be personal data. Thus they can be published or used outside the scope of data protection law, even if the original source contains personal data.[32] Although anonymization techniques can protect individual datasets, research has shown that linking datasets enables the reidentification of individuals in deidentified data and risks blurring the boundary between personal and nonpersonal data.[33] At the same time, anonymization techniques can

reduce the size and accuracy of datasets, affecting their value to third parties once published.[34]

Even when anonymization techniques can deidentify individuals, concerns are growing about the use of such data to identify groups of people who could be targeted for surveillance or discrimination (including groups defined by ethnicity, race, religion, or sexual orientation).[35] Data protection laws need to keep pace with technological efforts aimed at deanonymization.[36] Laws could require data users to adopt a holistic approach[37] to data protection that can be adapted to different risks from data uses,[38] including protecting data by design and default.

Adopting "data protection by design." Data protection by design embeds data protection practices into the initial design phase of data-driven products and services[39] through a combination of hardware and software features, legal and administrative provisions, and privacy-enhancing technologies (PETs) using encryption[40] and statistical techniques.[41] Such measures complement and enhance existing legal data protection in ways that reduce the risk of identifiability of data.[42]

Data protection by design has evolved from "privacy by design," which was first adopted as an international standard in 2010. It was later recognized by its inclusion in the Mauritius Declaration on the Internet of Things in 2014,[43] with a new International Organization for Standardization (ISO) standard under development.[44] The concept—originally developed in Canada[45]—has been integrated into data protection regulation and practice in the European Union,[46] as well as Australia (State of Victoria);[47] Hong Kong SAR, China;[48] and the United Kingdom.[49] Nevertheless, the Global Data Regulation Survey indicates limited uptake of data protection or privacy by design approaches. Less than 20 percent of the countries surveyed have adopted such requirements, ranging from 36 percent uptake in the high-income countries surveyed to negligible adoption in middle-income countries (figure 6.4). An interesting exception is Benin, which mandates "data protection by design" in its Digital Code Act.

PETs are often used to deidentify data at the source (for example, by relying on anonymization and aggregation) to reduce their identifiability. The result may be a trade-off between the level of data protection afforded and the resulting usefulness of the data (for data uses requiring granular or identifiable characteristics such as gender or age). Research showing the ease of reidentifying previously deidentified data (using only four data points[50] or when linking datasets) has highlighted the limitations of current anonymization methods and has prompted the development of new techniques.[51] Separately, the value of encryption-based PETs may be limited if law enforcement authorities argue that back doors should be included in these systems.

These limitations have also prompted the emergence of other mechanisms to protect personal data, including personal information management systems (PIMS) such as Safe Sharing sites[52] and personal data stores.[53] These tools can help users store, use, and manage how their personal information is shared with third parties. To address certain cybervulnerabilities and technical features of data protection by design and act as effective safeguards, PETs should be accompanied by supporting organizational and behavioral measures.[54]

Dealing with automated processing. The growing use of algorithms for automated processing of personal data can add significant value through the application of predictive analytics, but it poses additional regulatory and societal challenges. These include algorithmic bias, risks to personal data protection, and lack of transparency, accountability, and other procedural safeguards (such as redress) to ensure that decisions made on the basis of automated processing are conducted in compliance with due process.[55] Only about 30 percent of countries included in the Global Data Regulation Survey have put in place measures to restrict decision-making based on automatically processed personal data (figure 6.4). Among the relatively small number of countries whose laws address this, Côte d'Ivoire has included provisions in its data protection act that prohibit the use of automated processing of personal data in judicial decision-making to prevent bias.[56]

Automated processing of personal data in the criminal justice sector is an example of controversial public sector use of these technologies—especially those using facial recognition—that can perpetuate biases.[57] A 2016 study conducted in Oakland, California, found that, despite survey data showing an even distribution of drug use across racial groups, algorithmic predictions of police arrests were concentrated in predominantly African-American communities, creating feedback loops that reinforced patterns of structural or systemic bias in the history of police arrests.[58] Algorithms can also introduce racial biases when facial recognition algorithms are trained predominantly on data from Caucasian faces, significantly reducing their accuracy in recognizing other ethnicities.[59] Evidence suggests that

racial[60] and gender[61] bias in private sector uses of AI for decision-making is also prevalent.

Additional challenges within the public sector include a lack of transparency and accountability in the use of automated decision-making systems. Many of the technologies procured by public sector entities are developed by private sector corporations. Thus, the underlying algorithms may be subject to copyright or other IPRs that restrict the ability to undertake independent third-party audits. The use of such technologies by the public sector, without implementation of the appropriate audits and grievance redress mechanisms, may impair public trust in data processing by institutions and lead to discrimination or otherwise unfair decisions.

Because of these challenges, as the uptake in AI technologies and automated decision-making systems increases in both the public and private sectors, some principles for algorithmic regulation are emerging at both the national and international levels. Internationally, the focus has frequently been on developing guiding principles based on data ethics. For example, OECD and the Group of Twenty (G-20) published two closely related sets of principles on ethical AI in 2019 that highlight the need to ensure transparency, explainability, and inclusion of unrepresented or vulnerable groups in the design and implementation of AI systems.[62] Fulfilling this need will require significant capacity-building efforts to promote responsible use of AI in lower-income countries.

Principles grounded in data ethics can be applied to other types of data uses that may have important societal impacts. Human rights-based frameworks, for example, can provide useful guiding principles for responsible data use.[63] Some countries have made efforts to support transparency and accountability in the use of AI and automated decision-making systems in the public sector by publishing the source code of algorithms in public registers,[64] revising procurement rules, and developing charters,[65] regulations, or certifications.[66] In February 2020, a Dutch court ruled that an automated surveillance system developed to detect welfare fraud in the Netherlands (SyRI) violated human rights by not meeting a "fair balance" between its objectives and its risk to privacy. It then halted the system.[67]

Relying on competition and consumer protection laws. In countries where data protection legislation is not yet in place, other statutory instruments—notably, consumer protection and competition legislation—have been leveraged to protect the data rights of individuals, notwithstanding the rights' distinct legal focus. Under a rights-based approach, data protection law is generally aimed at achieving individual agency, whereas consumer protection law aims to promote economic fairness for consumers, and competition law strives for fairness among businesses. These approaches are complementary, but they are not an adequate substitute for the scope and protection of a rights-based data protection legal framework. Nonetheless, consumer protection agencies may have wider-ranging powers than data protection authorities,[68] equipping them to address some of the issues underlying misuse of personal data, such as unfair consumer practices or competition concerns (see chapter 7 for further discussion of data and competition issues).[69]

Safeguarding nonpersonal data

Safeguards for the domestic use and reuse of nonpersonal data revolve around the protection of intellectual property rights fit for the digital age, as well as cybersecurity measures. Various contractual elements affecting how entities use and reuse nonpersonal data (and even mixed data) are also relevant, including contracts themselves (terms and conditions, assignment of liability and remedies), as well as industry standards, codes of conduct, and audit requirements. Soft law tools include the use of standards to broker trust among entities exchanging data.

Nonpersonal data produced by the private sector can be protected under copyright, although copyright is limited to protecting creative expression, such as compilations, as opposed to raw data. Some governments have introduced innovations to overcome these limitations.[70] Observing that while the rights to data utilization may be controlled by contract but are not always specified in terms, Japan's Ministry of Economy, Trade and Industry updated application of the Unfair Competition Prevention Act to provide protection for industrial data by publishing guidelines along with model contract clauses for data transactions.[71] India's Ministry of Electronics and Information Technology published a draft governance framework for nonpersonal data, recommending clarifications on the scope, classification, rights of use of nonpersonal data, and creation of a nonpersonal data authority.[72]

Governments may also wish to establish rules to support the reuse of public sector data by preventing the private sector from setting excessively high prices for the use of licensed data-driven products and services developed using public sector, or otherwise "high value," data. One mechanism is to mandate firms to license such products on fair, reasonable, and non-discriminatory (FRAND) terms by considering

them "essential data infrastructure." Governments may, however, find that IPR protection of nonpersonal data conflicts with other policies that encourage the interoperability of data systems and the free reuse of datasets.

Protection of nonpersonal data under an IPR regime is currently more prevalent in upper-middle-income countries than in most of the low-income countries surveyed. Fifty percent of upper-middle-income countries protect nonpersonal data under their respective IPR frameworks. For example, Brazil's copyright law covers the use of databases containing "economic rights."[73] Similarly, in Bangladesh programming codes, data, and charts are deemed to be the property of the owner, as indicated in the 2000 Copyright Act.

Creating enablers for data sharing

This section examines a variety of enablers, including those related to electronic transactions (e-transactions), data sharing policies (including open data, access to information regimes, open licensing), and exceptions to the liability of data intermediaries.

Enablers are primarily analyzed according to the domain of the data—that is, whether data are generated or controlled, or both, by the public or private sector. This approach highlights the varying margin of control that governments have over these two types of data. For public sector data, governments can employ several policy and legal tools to directly mandate access to and sharing of data—indeed, some already do so for certain health, patent, and even airline passenger data. By contrast, most data transactions involving the private sector are based on voluntary contractual agreements. The government's role is largely limited to creating incentives to promote private sector data sharing. Although the discussion here deals mainly with domestic data transactions, many of the enablers can be adapted to cross-border data transactions (see chapter 7).

Across the 80 countries surveyed for this Report, just under half (47 percent) of the elements of a good-practice regulatory framework for enabling data use and reuse are in place. The scores range considerably, from 30 percent among low-income countries to 62 percent among high-income countries. Although Estonia and the United Kingdom stand out among the high-income countries surveyed for the most advanced enablers, their performance is matched in the middle-income group by Mexico. Several other low- and middle-income nations are also making progress establishing regulatory frameworks to enable data reuse, such as China, Colombia, Indonesia, and Nigeria.

Overarching enablers for electronic transactions

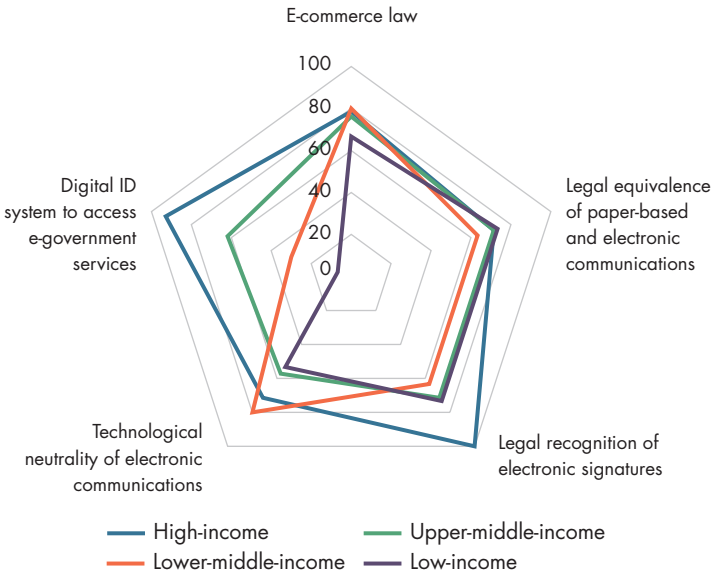
Many data uses or transfers are executed via electronic transactions. Individuals using their data to transact online need assurance that their data are being used in a safe and secure manner. Laws governing e-commerce and e-transactions provide an overarching legal framework that helps create trust in both public and private sector online data transactions, which, in turn, encourages use of data online.

Introducing e-commerce laws. A good-practice regulatory environment for electronic transactions begins with foundational e-commerce legislation, which is a prerequisite to the widespread use of more sophisticated online credentials. Such laws are relatively widespread; more than 70 of the countries surveyed, including about 70 percent of low-income countries surveyed, have such laws. And there is little variation across country income groups (figure 6.5). Legal recognition of electronic signatures is one of the few areas in which high-income countries remain far ahead of low- and middle-income countries.

Establishing legal equivalence of paper-based and electronic communications. In a legal framework, the central issue is to establish that a data transfer will not be denied legal value merely because it is done electronically—that is, the online transaction, contract, or communication has legal equivalence to physical transactions, and electronic evidence has probative value.[74] For example, electronic contracts and signatures are given the same legal value as a wet ink signature on a paper contract, and digital evidence has the same value as physical evidence.[75] The majority of surveyed countries' e-commerce legislation includes such provisions (figure 6.5), an unsurprising finding given that model laws on e-commerce were promulgated in the late 1990s.[76] For example, provisions enabling e-transactions are found in Morocco's Law No. 53-05 (2007), and good-practice provisions are embedded in Thailand's Electronic Transactions Act (2019 amendments).

Authenticating parties to an online transaction. Special legal treatment surrounds the manner in which parties to an online transaction are authenticated. Most laws governing e-transactions take a layered approach to the digital authentication of parties to a transaction, with built-in recognition that certain types of online transactions require greater degrees of reliability about the identity of parties, while others

Figure 6.5 Adoption of e-commerce and related legislation is widespread across country income groups



Source: WDR 2021 team, based on World Bank, Global Data Regulation Survey, https://microdata.worldbank.org/index.php/catalog/3866. Data at http://bit.do/WDR2021-Fig-6_5.

Note: The figure shows the percentage of countries in each country income group that had adopted good-practice legal and regulatory frameworks for e-commerce as of 2020.

require lower levels of assurance. Some—such as land transactions and certain family law matters, including marriage and divorce—are generally outside the scope of these laws because of the sensitive nature of the transaction. For transactions requiring a high level of assurance, public or private key infrastructure is often recognized in e-transaction laws as providing robust authentication, and it is backed up by a digital certification process.[77] Other trust services may also be specified as a basis for verifying and validating electronic signatures, seals, or time stamps; verifying and validating certificates to be used for website authentication; and a range of activities related to data transfers.[78]

Introducing digital identification. An important tool for authentication of parties to a digital transaction is a trusted digital identification system with widespread coverage, allowing individuals to securely prove their identity in online settings. Currently, an estimated 1 billion people worldwide do not have government-recognized proof of their identity (and many more do not have the means to securely and reliably prove who they are in the digital world).[79] Although the use of digital identity verification and authentication tools is on the rise, driven in part by advances in connectivity as well as growth in digital payments and services,[80] fewer than half of surveyed countries have government-recognized digital identification systems that would enable people to remotely authenticate themselves to access e-government services. Those that do are mainly higher-income nations (figure 6.5).

Ensuring technical neutrality of online systems. E-transaction laws should be principle-based and technology-neutral so that they accommodate a wide range of technical solutions and avoid requiring specific authentication technologies to the exclusion of others. Such requirements avoid capture of the e-transaction or authentication market and help laws adapt as technologies evolve.[81] Technology neutrality is also a feature of digital identity programs and of some digital identity laws.[82]

Enabling reuse of public intent data

The challenges with sharing and reusing public sector data abound. They include barriers to the real-time provision of data; data not being shared or published in reusable formats (standardized and machine readable with metadata); and data not being provided at reasonable cost. Usage is also affected by the quality or relevance of the data being shared. Political economy factors, including the absence of a data sharing culture in public administration and lack of coordination among government entities, can further impede the exchange of public sector data (see chapter 8).

Overcoming these challenges can yield considerable returns. An impact assessment of the 2003 Directive on the Reuse of Public Sector Information found that in the European Union the direct economic value of public sector information was €52 billion in 2017, potentially rising to €194 billion by 2030.[83] In recognition of such potential value, national governments have ramped up efforts to use policy, legal, and regulatory tools to mandate data sharing within and beyond the public sector.

A good-practice regulatory environment for enabling reuse of public sector data would include foundational legislation on open data and access to information, as well as digital identity verification and authentication; a data classification policy; adoption of syntactic and semantic interoperability; and user-friendly licensing arrangements. The surveyed countries have adopted about half of such good practices, ranging, on average, from less than 30 percent by low-income countries to two-thirds by high-income countries (figure 6.6).

Legislation to promote and regulate the publication and use of public sector data (open government

data) can be passed as stand-alone open data acts, such as in the Republic of Korea and Mexico; embedded in other related legislation, such as the laws mandating data sharing in Australia,[84] India, and the United Kingdom;[85] or through broader e-government omnibus legislation, such as France's Law for a Digital Republic.[86] The matter can also be tackled at the supranational level, such as through the European Union's Open Data Directive of 2019 (replacing the Public Sector Reuse Directive of 2003), which includes a list of "high value datasets"[87] to be published at no charge as key inputs to the development of AI.

Open data policies or laws and access to information (ATI) legislation (also known as right to information or freedom of information) play complementary roles as enablers for the use and sharing of public sector data. Open data policies or laws require public disclosure of data as the general rule (ex ante disclosure) rather than waiting for an individual request for access to information (ex post disclosure).[88] In countries that have passed open data policies without any legal foundation, the publication of open government data relies on the cooperation of holders of public sector data to publish their data. By contrast, ATI legislation provides citizens and firms with a legally enforceable right to compel disclosure.[89]

Open Barometer, an organization that compiles a global measure of how governments are publishing and using open data for accountability, innovation, and social impact, recommends aligning access to information and open data. This alignment would entail amending ATI laws to provide for proactive disclosure of data and mandating that nonpersonal data will be open by default, available in machine readable formats, and published under an open license to enable reuse outside government.

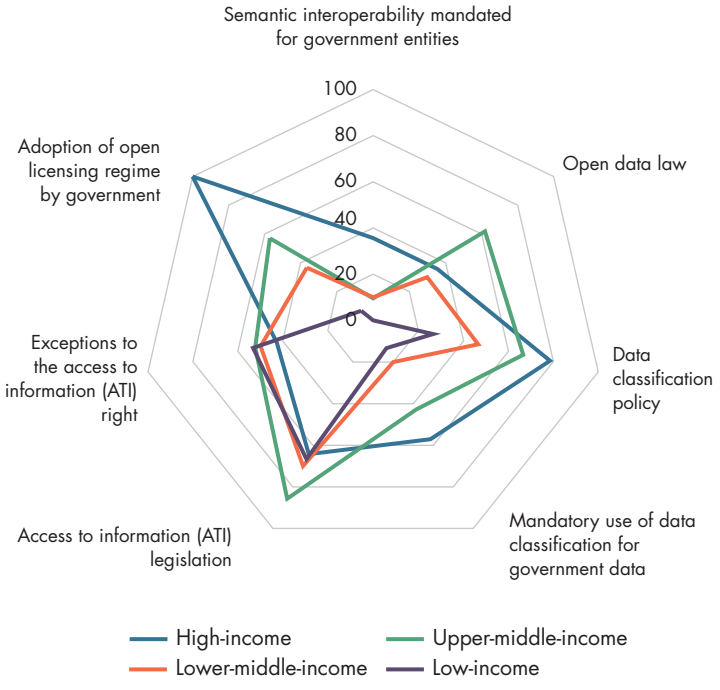
About one-third of surveyed countries have open data legislation, and more than 70 percent have ATI legislation (figure 6.6). Whereas ATI legislation is widespread in countries across all stages of development, adoption of open licensing regimes is more common in high-income countries.

Establishing open data policies. A country's public sector data being prepared for publication can be classified on a spectrum from closed to open. According to the Open Knowledge Foundation, for data to be considered open it must be "freely used, re-used and redistributed by anyone—subject only, at most, to the requirement to attribute and sharealike."[90] Open data are thought to be the most decisive approach governments can use to enhance access to public sector data and enable their reuse by third parties to create value.[91] According to the Open Data Institute, key elements of a robust data policy include a clear definition of open data and a general declaration of principles that should guide the publication and reuse of open data.[92]

Geospatial and transportation data are often prioritized for publication by governments under open data initiatives.[93] However, certain categories of data may not be suitable for publication as open data, including personal data and data with national security implications. Care must be taken to ensure that personal data are not published on open data portals without adequate protective measures and a conscious assessment of the associated risks. A data protection impact assessment can be used to evaluate the risks of data processing and ensure that data are adequately safeguarded before being shared.[94]

As open data systems mature, governments should move from merely promoting access to data to facilitating use of data. A key enabling reform is ensuring that data and metadata are "open by default," available

Figure 6.6 Regulations enabling access to and reuse of public intent data are unevenly developed across country income groups



Source: WDR 2021 team, based on World Bank, Global Data Regulation Survey, https://microdata.worldbank.org/index.php/catalog/3866. Data at http://bit.do/WDR2021-Fig-6_6.

Note: The figure shows the percentage of countries in each country income group that had adopted good-practice legal and regulatory frameworks to enable access, use, and reuse of public intent data as of 2020.

in a machine readable format and by bulk download or via application programming interfaces (APIs)—computing interfaces and code that allow data to be readily transmitted between one software product or application and another. A survey conducted by the Open Data Barometer found that less than 10 percent of governments that have established open data portals include a provision for data to be open by default. Moreover, only half of the datasets published are in a machine readable format, and only one-quarter of datasets have an open license.[95]

Ensuring unified data classification standards. A key enabler of data reuse is a data classification policy that categorizes types of data according to objective and easily implementable criteria across the different stages of the data life cycle.[96] Data classification policies typically entail categorizing data according to their sensitivity (such as classified, confidential, or business use only). Although data classification policies are found in more than half of the countries surveyed (figure 6.6), their practical effects are limited because in less than one-third of countries is the application of data classification policies mandatory for government database applications or document management systems.

Restricted data (data that cannot be published as open data) could possibly be shared bilaterally by agreement (such as with memoranda of understanding). Alternatively, innovative mechanisms, including data pools and data sandboxes, allow data to be accessed and processed in a controlled environment, subject to specific restrictions on data use. For example, data could be analyzed at a secure data repository (whether virtual or physical) but not taken off-site.[97]

Allowing access to information. ATI legislation is a key complementary enabler for increasing access to public sector data that have not been published on an open data platform. Such legislation provides the legal means for enforcement of public sector disclosure.[98] As with open data legislation, ATI legislation can be more or less effectively implemented, depending on how broadly the exemption categories for disclosure are drafted or interpreted and how restrictively data classification policies are applied at the working level. If government entities claim that much of their data are "sensitive" and therefore fall under one of the exceptions for disclosure under ATI statutes, then the usefulness of such legislation for enabling public data access may be limited. This concern is warranted because nearly half the countries included in the Global Data Regulation Survey—across the income spectrum—have placed significant exceptions on an individual's rights to access public information under such laws (figure 6.6).

Another limit to the impact of ATI legislation is its scope of application, which is necessarily limited to public sector data. Open data policies, although originating in the public sector, can be voluntarily adopted by the private sector. However, there is no general legal equivalent to ATI requests to compel the disclosure of private sector data. Currently, the majority of private sector data sharing is undertaken on a contractual basis. Certain experts have argued that expanding the scope of laws mandating access to private sector data, consistent with competition law, could be the "next frontier in data governance."[99]

Promoting interoperability of data and systems. For the value of data—including open data—to be fully harnessed, legislation must go beyond promoting access to data and ensure that data can be used more effectively by combining or linking datasets. Doing so requires provisions governing the interoperability of data (and metadata) and their quality, as well as the modalities under which data should be published. These good-practice characteristics include publishing data in a machine readable format (under FAIR principles that govern the findability, accessibility, interoperability, and reuse of data)[100] and ideally via APIs.[101] Interoperability of data and systems can be supported by adopting harmonized standards—ideally, open standards. Open standards are often determined by sectoral or international standard setting organizations (SSOs) in order to support the interoperability of data and systems within a particular market or sector. They are therefore designed collaboratively based on user needs.[102]

Public intent data should also be published under an open license and at no charge or at a marginal price to cover the costs of dissemination or reproduction.[103] Nearly 48 percent of the surveyed countries have adopted some form of open licensing regime for public intent data. All the high-income countries covered in the survey have done so, compared with about 40 percent of middle-income countries. Other countries, such as Jordan and Mauritius,[104] have adopted Creative Commons Attribution 4.0 International Licenses for government datasets released as open data. In Jordan, datasets published by the government are open to all and licensed under a Jordanian Open Government Data License, which allows the use, reuse, and sharing of data, in compatibility with the Creative Commons (CC-BY) license.[105] To ensure that data prioritized for publication meet the needs of nongovernmental actors in the private

sector and civil society, these decisions should be guided by consultations with multiple stakeholders (see chapter 8).

Enabling access to and the seamless transfer of public sector data between different entities within the public sector and with end users (including individuals and businesses) requires ensuring the interoperability of information technology (IT) systems (including platforms) and data (syntactic and semantic interoperability). As defined by ISO, syntactic interoperability enables "the *formats* of the exchanged information [to] be understood by the participating systems," while semantic interoperability enables the "meaning of the data model within the context of a subject area to be understood by the participating systems."[106] Effective data and systems interoperability requires the implementation of several technical protocols and a government interoperability platform.

In addition to technical enablers for interoperability across the whole of government, an enabling legal and regulatory framework is often required. This framework mandates the use of the government's interoperability platform and data exchange protocols, ensuring that all government entities connect to and use the platform as a vehicle for exchanging data. Very few countries surveyed have adopted a full range of common technical standards (such as the FAIR principles) that enable the interoperability of systems, registries, and databases (figure 6.6). Estonia is among the few countries surveyed that has established standards for open APIs for government to government (G2G), government to business (G2B), and government to consumer (G2C) services; standardized communications protocols for accessing metadata; and developed semantic catalogues for data and metadata.

A distinct advantage of implementing interoperability is the possibility of applying the once-only principle to access to data, which reduces the administrative burden. Citizens and businesses are asked to provide their data only once, thereby requiring public sector entities to internally share and reuse data—with the appropriate safeguards—in the provision of administrative services. Because the risk of data breaches and misuse increases when data are stored in centralized or decentralized but linked repositories, the once-only principle should be complemented with robust legal and technical data protection as well as cybersecurity and cybercrime safeguards, implemented in a citizen-centered and trustworthy manner, with sufficient capacity for implementation (see chapter 8).[107] This once-only principle was integrated into the European eGovernment Action Plan (2016–20) for implementation across the European Union,[108] with the intention of enabling both domestic and cross-border interoperability. It is also one of the pillars of the 2015 Digital Single Market strategy[109] and The Once-Only Principle Project (TOOP),[110] which has been piloted under the European Union's Horizon 2020 framework.[111] At the national level, Austria, Belgium, Denmark, Estonia, the Netherlands, Portugal, and Spain have integrated the once-only principle into domestic law for application across government or on a sector basis.[112]

Enabling reuse of private intent data

The majority of business-to-business (B2B) and business-to-government (B2G) data transactions are governed by bilateral data sharing agreements sourced in contract law.[113] Consequently, policy and legal interventions to encourage access to private sector data focus on mitigating the legal and technical challenges that discourage the use and sharing of data by private sector entities. Governments also maintain a greater margin of control over private sector data transactions involving personal data, which are subject to personal data protection and privacy legislation (or competition and consumer protection laws).

As appreciation has grown of the strategic value of private sector data for enabling evidence-based policy making and promoting innovation and competition in key sectors (see chapter 4), some governments have enacted legislation mandating the sharing of private sector data deemed to be in the public interest and whose voluntary sharing by the private sector would, otherwise, have been too costly to incentivize.[114] Many of the sectors prioritized by such legislation (including utilities and transportation) are considered to be particularly relevant for the development of AI.

At the European level, the 2019 EU Open Data Directive[115] requires the European Commission to adopt a list of high-value datasets to be provided free of charge, in machine readable formats, via APIs, and where relevant, via bulk download. These datasets, considered to have "high commercial or societal potential," include geospatial data, Earth observation data, meteorological data, data about corporate ownership, mobility data, and data from publicly funded research projects.[116] At the national level, France's Law for a Digital Republic (2016) includes provisions mandating making private sector data available according to open standards for the creation of "public interest datasets."[117] Another relevant example is the UK

Digital Economy Act (2017), which enables researchers to gain access to deidentified data for research purposes.[118] At the subnational level, cities such as New York, San Francisco, and São Paulo have also made legal attempts to promote public-private data sharing by requiring certain private sector platforms to share their commercial data for regulatory purposes and to spur the development of smart cities.[119]

A good-practice regulatory environment for enabling reuse of private sector data encompasses data portability and voluntary licensing of access to essential data (figure 6.7). On average, surveyed countries have adopted less than 20 percent of such good practices for enabling private sector reuse of data, which is less than half the level of uptake found for enablers related to public sector data.

Promoting open licensing. Licensing regimes, which provide permission to use an otherwise proprietary dataset, can be effective enablers of innovation and competition. They can encourage holders of data-related intellectual property rights to invest in products and markets, knowing that they can control access to licensed products and receive returns on their investments.[120] Licensing of intellectual property rights is often voluntary, but in some cases it is implemented on a compulsory basis by regulators or industry participants to avoid market distortions.[121] Voluntary licensing on FRAND terms can be a useful mechanism in enabling the development of open standards because the terms allow companies to share technology and data.[122] The adoption of such licensing regimes, however, remains rare, especially in low- and middle-income nations (figure 6.7). Korea and the United Kingdom are among the few surveyed countries that have done so.

A range of open licenses are available for use with data. Open data licenses (Open Database Licenses, or ODbLs) provide users with the legal rights to freely share, modify, and use a database without regard to copyright or other intellectual property rights or limitations around data ownership. These license agreements are published by the Open Data Commons, which makes available a set of legal tools and licenses to help users publish, provide, and use open data.[123] The ODbL license sets out user rights, establishes the correct procedure for attributing credit, and specifies how to modify data to facilitate their sharing and comparability. Another form of open license for data is issued by Creative Commons, an international network devoted to educational access and expanding the range of creative works available for others to build on legally and to share.[124] Under the license, any person can use, copy, publish, distribute, transmit, or process the data and make them available to third parties. They can also develop new derivatives of the data by combining them with other data or using them in a product or service, as long as they are attributed to the publisher(s) using a specified statement.[125]

Requiring data portability. Voluntary data transactions between parties are greatly facilitated by data portability. The right to personal data portability is designed to facilitate data transfers with the aim of increasing an individual's choice and control over data about them. More fundamentally, the right to personal data portability is aimed at "rebalancing the relationship" between data generators/providers and data controllers (including data users and platforms) by mitigating the risk of locking in consumer data. On a more systemic level, this right is intended to foster competition between companies.[126]

Portability can be broken down into three distinct rights: first, to receive a copy of the data provided by the data generator to the data collector or user (including data consumers and platforms); second, to transmit data to another data collector/user;

Figure 6.7 Adoption of enablers for sharing private intent data lags those for public intent data across country income groups

Source: WDR 2021 team, based on World Bank, Global Data Regulation Survey, https://microdata.worldbank.org/index.php/catalog/3866. Data at http://bit.do/WDR2021-Fig-6_7.

Note: The figure shows the percentage of countries in each country income group that had adopted good-practice legal and regulatory frameworks to enable access to, sharing, and reuse of private intent data as of 2020. FRAND = fair, reasonable, and non-discriminatory; ID = identification.

and third, to request a direct transfer from one data collector/user to another.[127]

Although data portability rights extend to the raw data provided by the data subject (interpreted to include observed data), they do not appear to extend to inferred data (based on drawing inferences from the raw data provided), which are increasingly being used to develop AI.[128] Enabling the direct transfer of (personal or nonpersonal) data to another provider requires that the source and host data formats and systems are fully interoperable through the implementation of APIs.[129] At present, interoperability is encouraged, not mandated, by the GDPR[130] and EU regulations on the free flow of nonpersonal data.[131] Alternatives to direct portability include storing personal data in personal information management systems,[132] although their uptake is limited.[133]

In the European Union, the right to personal data portability is mandated by Article 20 of the GDPR and considered one of its most significant innovations.[134] Little more than 10 percent of countries surveyed have enacted data portability rights for individuals. By contrast, the portability of nonpersonal data is not mandated, but only encouraged as a means of promoting competition and enabling the development of competitive sectors using AI and big data.[135]

Individuals' ability to enforce their right to data portability can in practice be supported by requiring data to be transferred in a standard machine readable format. The surveyed countries that grant individuals data portability rights all include formatting requirements to support data portability (figure 6.7). For example, in the Philippines the 2012 Data Protection Act grants data portability rights to data subjects and empowers the National Privacy Commission to specify the format and technical requirements to enable data portability.[136] Using a somewhat different approach, Australia created a specific "consumer data right" in August 2019[137] to enable data portability through its Competition and Consumer Act 2010.[138] The act follows a phased sectoral approach to implementation,[139] which enables common standards to be adapted to sector-specific needs while being made publicly available on the open-source platform GitHub.[140]

Despite these advances, technical limitations and legal uncertainties challenge effective enforcement of data portability rights. At the same time, cybersecurity risks, such as improper access or identity theft, could increase if portability is not accompanied by robust security measures.

In the absence of specific laws or regulations mandating interoperability and portability standards, some private sector actors have developed their own mechanisms. One example is the collaborative Data Transfer Project.[141] Data format standardization is a key component of enabling data portability in practice: the right to data portability cannot be exercised if data are not downloaded in a format common to other service providers. In practice, despite the source code and APIs being open source, the leadership of this project raises broader questions about the first mover advantage that Big Tech companies have in setting de facto standards and markets for B2B data sharing between platforms.

Using APIs to enable effective interoperability and portability. APIs can be used to either enable data sharing (such as through open APIs) and portability or limit access to data, depending on how they are designed.[142] Although APIs are technical in nature, technolegal frameworks can be developed to determine access and control rules for third parties. These rules can include setting controls to ensure the syntactic and synthetic portability of data; the identity of the API users; the type and amount of data transacted; and the controls on the identifiability of data.[143] APIs designed with access and control mechanisms that enable the selection of a limited amount of data can provide users with more flexibility than if they downloaded bulk data.[144] That said, because APIs can expose data to unauthorized access during data transfers, they may prove challenging to use effectively in lower-middle-income countries that do not have sufficient technical capacity to respond to cybersecurity risks.

Fully leveraging APIs to enable effective interoperability and portability requires ensuring that they are developed according to common standards. These standards can be developed through regulation or by industry, based on a multistakeholder approach. Examples of successful initiatives include the Berlin Group, which has developed common API standards for the European banking industry.[145] Cases from the financial services sector (such as the UK Open Banking Initiative and implementation of the European Union's Second Payment Service Directive) may provide helpful lessons for the effective implementation of these mechanisms as enablers for data reuse and sharing.

Forging data partnerships. An alternative modality for private sector data sharing is through data public-private partnerships (PPPs) entered into on mutually agreed contractual terms between private sector entities or between government and businesses. For example, the traffic application Waze has partnered

with more than 1,000 cities and other local public sector entities through its Connected Citizens Program[146] to exchange traffic data and derive insights to inform mobility projects, manage traffic and congestion, support emergency response, and share data with citizens through a cloud-based platform.[147]

Data partnerships pose several challenges. Partnerships between large companies and small and medium enterprises may raise concerns about fairness because of asymmetries in information or market power. Partnerships between public and private entities may lead to conflicts of interest because of the government's dual role as data user and data regulator.[148] In either case, partnerships may create uncertainties around the allocation of the legal liability associated with the use of the data, as well as potential compliance costs due to lack of harmonization of legal frameworks applicable to both parties.[149] Some of these risks can be mitigated by developing contract guidelines or standard contractual terms to harmonize provisions and rectify information asymmetries. Some public sector initiatives have attempted to develop such standard terms to promote data sharing.[150]

Not all data sharing partnerships are designed for profit. Some businesses provide their data and digital tools at no charge to governments, academia, and nongovernmental organizations for "social good." Data philanthropy,[151] particularly in the area of big data, has enabled the World Bank,[152] together with UN agencies—the World Health Organization (WHO), United Nations Development Programme (UNDP), World Food Programme (WFP), and United Nations Children's Fund (UNICEF)—and others, to leverage companies' data stock and digital capabilities to fully exploit the value of data for development, while benefiting the private sector through positive externalities.

Limiting intermediary liability. One of the great enablers of the flow of data across the internet are rules limiting the liability of intermediaries for content that flows over their platforms. The intermediary liability concept has roots in US telecommunications law dating back to the 1930s,[153] and it has been informed by subsequent US case law.[154] Crucially, this exemption from liability was extended to "interactive computer services" (internet service providers) in Section 230 of the 1996 amendments to the Communications Act of 1934[155] and in the Digital Millennium Copyright Act.[156] The advent of data platform business models has led to growing requests from users for the "take-down" of their personal information and has triggered an ongoing debate between privacy advocates and Big Tech about responsibility for fundamental issues of freedom of expression and transparency of knowledge. Liability exemptions have been criticized as harboring defamatory conduct, encouraging harassment online, and undermining attempts by law enforcement to attribute conduct to specific individuals.[157] Nevertheless, freedom of expression advocates continue to support shielding intermediaries from liability.[158] The rapidly changing landscape is creating significant regulatory uncertainty for Big Tech firms (see the overview and chapter 1 for a discussion on the broader policy considerations relating to content moderation and mis/disinformation).

Recommendations for crafting a holistic legal framework

Any new social contract on data must rest on the foundation of a comprehensive legal and regulatory framework that helps build trust between stakeholders, integrating both safeguards and enablers. As the results of the Global Data Regulation Survey suggest, the development and robustness of different aspects of the legal and regulatory framework are quite uneven, with relatively consistent patterns across country income groups (table 6.1). These divergences may be exacerbated by differences in implementation. E-commerce legislation is the only area in which all country income groups are doing comparatively well. Development is at an intermediate level in areas such as enabling reuse of public intent data, safeguarding both personal and nonpersonal data, protecting cybersecurity, and combating cybercrime. By far the weakest area of performance of the surveyed countries is enablers for private intent data. Overall, the average scores of high-income countries are not very high in absolute terms, warranting an advanced (green) classification in table 6.1 in only one case. And the score differential between high- and low-income countries is relatively small (rarely more than 30 points). Both findings indicate the novel challenges of developing a sound data governance legal framework and the significant progress all countries need to make.

To fill the many remaining gaps in the legal framework and further strengthen existing provisions, this Report offers several recommendations. Overall, the underlying legal framework needs to be approached holistically. Although different elements of the legal framework can be viewed in a modular fashion, the elaboration of particular laws needs to touch on all critical aspects. The crafting of such a coherent legal framework should take into account both evolving best practices and local conditions based on robust

Table 6.1 Certain elements of the regulatory framework are much better developed than others, but performance is generally low

Average score, by country group	Safeguards			Enablers		
	Cybersecurity and cybercrime	Personal data	Nonpersonal data	E-commerce and e-transactions	Public intent data	Private intent data
High-income	73	59	43	86	69	30
Upper-middle-income	57	46	29	74	62	20
Lower-middle-income	55	43	38	72	44	15
Low-income	39	31	47	59	28	3
Global	**56**	**44**	**38**	**73**	**50**	**17**

Source: WDR 2021 team, based on World Bank, Global Data Regulation Survey, https://microdata.worldbank.org/index.php/catalog/3866.

Note: The table shows the average score for good-practice data governance by theme across country income groups as of 2020. Colors refer to the level of the regulatory framework: ■ = advanced level (scores of 75–100); ■ = moderate level (scores of 50–75); ■ = evolving level (scores of 25–50); and ■ = basic level (scores below 25).

stakeholder consultation. There is no one-size-fits-all solution.

Recommendations for strengthening safeguards

Adopt and implement personal data protection legislation. One of the biggest contributors to the trust framework is the adoption of personal data protection legislation following a rights-based approach. For countries that lack data protection legislation or enforcement agencies, the existing consumer protection legislation and competition law can be leveraged to remedy certain manifestations of the misuse of personal data. Although such legislation and laws may be helpful, their scope of application is limited, making them complements to, not substitutes for, personal data protection legislation.

Introduce more meaningful models of consent. Traditional approaches to consent, developed in an analog age, are an increasingly uncomfortable fit in the modern digital age. Furthermore, in lower-income countries, where literacy challenges continue to affect a significant share of the population, reliance on "consent," as traditionally applied, will continue to be problematic as more people access the internet and permit their data to be used and reused. To ensure that consent remains a meaningful legal basis for using data, new models should be seriously considered, including those that shift responsibility for data protection from individuals to the collectors and users of the data.

Expand protection to mixed data and group privacy. New data uses, fueled by innovative analytical techniques and the growth of algorithm-based technologies such as big data and the Internet of Things, are blurring the distinction between personal and nonpersonal data. At present, only personal data fall within the scope of most current data protection laws, while anonymized personal data are considered nonpersonal data. In view of the ease of reidentifying and linking datasets, which opens the door to deriving sensitive or discriminatory insights from the processing of nonpersonal data, policy makers should consider expanding the scope of data protection legislation to protect such mixed data. A related issue is that current provisions for personal data protection, which focus on the individual, do not preclude the identification and potential misuse of data attributes pertaining to homogeneous groups (including those defined by ethnicity, race, religion, or sexual orientation). These protections are particularly important in complex or fragile sociopolitical environments or emergency contexts because of the increased risk of misuse of such data for targeting or surveillance.

Adopt data protection by design and default. Privacy-enhancing technologies are important complements of data protection legislation, allowing privacy to be embedded in data-driven products and services right from the design phase. These standards can play a valuable role in safeguarding fundamental data rights in contexts in which weak institutional capacity diminishes the legal enforceability of those rights. However, for technical mechanisms to have teeth, they must be underpinned by a robust legal framework that creates the rights and limits on use that privacy-enhancing technologies reinforce. Because of the utility of data protection and privacy by design, policy makers should consider building more of these

requirements into their regulatory frameworks, while maintaining technological neutrality.

Prioritize cybersecurity measures. Protecting individuals' and groups' rights in data is one thing; protecting the infrastructure and systems over which those data flow—cybersecurity—is another. From a legal perspective, these protections are gained by adopting cybercrime legislation that balances security concerns with other fundamental rights. Too few countries have adopted serious legal provisions to ensure cybersecurity, leading to mounting social and economic risks. This gap should be addressed as a matter of urgency.

Recommendations for strengthening enablers

Build a robust yet flexible foundation for electronic transactions. Digital transactions should be granted legal equivalence to the analog variety, with limited exceptions. Robust authentication should be technology neutral to ensure a level playing field for a wide variety of approaches to authenticating transactions and related trust services.

Make data open by default and easy to access. Countries should strengthen open data policies by calling for open-by-default approaches to public sector data through legislation across the whole of government. Datasets to be published should be prioritized using input from end users. End users should not be charged (or should pay a limited price) for public intent data.

Consistently apply reasonable norms for data classification. Implementation of open data policies or laws requires the consistent application of clear, reasonable data classification policies.

Adopt open standards and sharing-friendly licenses. Policy makers should strengthen open access to public intent data, including adoption of open standards and sharing-friendly licenses.

Strengthen access to information provisions. Access to information legislation should be expanded to cover the proactive and transparent disclosure of nonsensitive data. Exceptions to disclosure will be necessary and should be proportionate. ATI laws should provide for regular public disclosure of ATI requests received and rejected, and justification for any rejection, ideally on an open platform.

Promote the interoperability of data and systems. Improving the use and sharing of data will rely on developing and applying unified technical standards to support the interoperability of data and systems. Interoperability of systems entails adoption of common technical protocols and a government interoperability platform. Data can be made interoperable by ensuring that they are classified and processed according to common standards and published in a machine readable format.

Support data portability. The right to data portability should be strengthened by requiring data to be in a structured, commonly used, and machine readable format. Interoperable data and systems can help achieve continuous data portability, where proportionate and technically feasible. As an alternative or complement to direct portability, personal information management systems can help users receive and manage their data, but their uptake is currently limited. The enforcement of data portability rights depends on adequate market competition, enabling users to switch providers. For data portability to be meaningful, there is also a need to address the lack of clear understanding of these rights by data subjects, as well as the implementation challenges faced by micro, small, and medium enterprises.

Promote sharing of private intent data. Governments can incentivize the sharing of private sector data by promoting data sharing agreements and enhancing intellectual property rights. Together, these measures can help reduce incentives for data hoarding and leverage the reusability of data. In the case of public interest data, and particularly under emergency situations, governments should increasingly consider mandating private sector data sharing, subject to suitable conditions and safeguards.

A maturity model for strengthening the legal and regulatory framework

The urgency of applying these measures will depend on how far a country's legal and regulatory framework for data has evolved. Countries should develop sound, comprehensive policies based on best practices adapted to their circumstances. Building on this foundation, countries should then enact robust legislation buttressed by multistakeholder consultation, followed by clear time-bound implementation procedures to ensure accountability. The identified measures can tentatively be mapped onto the maturity model framework summarized in table 6.2. Although certain safeguarding and enabling elements are considered foundational, the ability to build an effective legal regime for trusted data use is dependent on ensuring that the overall framework is both internally coherent and aligned with the country's policy orientation, data culture, and social contract on data.

Table 6.2 Recommendations organized according to a maturity model based on data safeguards and enablers

Stage of country's data system	Safeguards	Enablers
Establishing fundamentals	Conduct a baseline needs assessment. Develop a comprehensive policy framework based on best practices that does the following: • Safeguards personal, nonpersonal, and evolving categories of data and promotes greater equity around data • Enhances the security of systems and infrastructure that protect against misuse of data • Expands individuals' agency and control over their personal data • Promotes certainty and predictability, integrating the fundamental safeguards discussed in this chapter such as data protection and cybersecurity.	Conduct a baseline needs assessment. Develop a comprehensive policy framework based on best practices that enables the use and sharing of data for development purposes, ensuring access, openness, interoperability, portability, predictability, and transparency, while integrating the fundamental enablers discussed in this chapter, such as electronic transactions.
Initiating data flows	Elaborate a legal framework that embodies policy prerogatives that include: • Personal data protection • Promotion of cybersecurity and combating of cybercrime • Regulation of competition • Provisions in the legal framework to provide for establishment of the relevant enforcement institutions.	Elaborate a legal framework that embodies policy prerogatives that include: • Legal recognition of e-transactions • Access to information • Intellectual property rights for nonpersonal data • Openness of public intent data, including the use of licenses that encourage data sharing • Data classification principles.
Optimizing the system	Promote awareness of safeguards: • Domestically, through adoption of data protection by design and default, together with associated cybersecurity measures • Internationally, through cross-border interoperability of data protection standards • Address more complex issues such as mixed data and group rights • Ensure that the capacity of the institutions responsible for overseeing these activities is sufficient • Establish metrics to monitor and evaluate the implementation and enforcement of these policies and laws.	Consider issues such as data portability and increasing incentives around sharing of private intent data. Ensure that the capacity of the institutions responsible for overseeing these activities is sufficient. Establish metrics to monitor and evaluate the implementation of these policies, laws, and institutions.

Source: WDR 2021 team.

Notes

1. Gellman (2013).
2. Confessore (2018).
3. A framework for data protection existed in the EU prior to the GDPR—the 1995 Data Protection Directive. Because a directive requires incorporation into domestic law, several European countries adopted their own data protection regimes, in some cases with even more stringent protections (such as Germany). However, adoption of the GDPR is a significant evolution in three key dimensions. First, as a regulation that applies directly to all EU members, it has harmonized data protection law across the EU. Second, it has supported enforcement through the introduction of significant fines. And, third, it has applied extraterritorially to cross-border data transactions involving data subjects in the EU.
4. Attorney General's Office, California Department of Justice, California Consumer Privacy Act (CCPA), https://oag.ca.gov/privacy/ccpa.
5. China's revision of its civil code will enter into force in 2021. Articles 1032–1039 grant certain rights to individuals. These provisions may be superseded by the expected introduction of a new law on protection of personal information. See, for example, Dong (2020) and Fang, Bigg, and Zhang (2020). China also published for consultation a draft law on personal data protection that in many respects mirrors provisions of the GDPR (Zhang and Yin 2020).

6. See Fisher and Streinz (2021) and Lessig (1999).
7. Personally identifiable information refers to information that can be used to distinguish or trace the identity of a data subject. Examples of such information are the subject's name, national identity number, or biometric records, alone or when combined with other personal or identifying information that is linked or linkable to a specific data subject, such as date and place of birth or mother's maiden name.
8. PMC (2019).
9. A regulatory impact analysis (RIA), also known as a regulatory impact assessment, is defined by the Organisation for Economic Co-operation and Development (OECD) as "a systemic approach to critically assessing the positive and negative effects of proposed and existing regulations and nonregulatory alternatives. As employed in OECD countries it encompasses a range of methods. It is an important element of an evidence-based approach to policy making" (OECD, "Regulatory Impact Analysis," https://www.oecd.org/regreform/regulatory-policy/ria.htm). According to data from the World Bank's Global Indicators of Regulatory Governance (GIRG), 86 out of 186 countries surveyed carry out RIAs on either a regular or a semi-regular basis (World Bank, Global Indicators of Regulatory Governance [dashboard], https://rulemaking.worldbank.org/). However, although most high-income countries carry out RIAs (45 out of 59, or 76 percent), only 12 percent of low- and middle-income countries do so. Moreover, even though all OECD high-income countries except for Italy and Chile have developed specific RIA guidelines, only three countries in Sub-Saharan Africa (Kenya, South Africa, and Uganda) have set requirements. For more details, see Deighton-Smith, Erbacci, and Kauffmann (2016); ITU (2014); World Bank (2018); World Bank, "Key Findings," https://rulemaking.worldbank.org/en/key-findings.
10. Chen (2021). To access the World Bank's Global Data Regulation Survey and its results, see https://microdata.worldbank.org/index.php/catalog/3866.
11. COE (2018).
12. See, generally, page 70 of World Bank and United Nations (2017).
13. World Bank and United Nations (2017).
14. World Bank and United Nations (2017).
15. In the absence of dual criminality, if an activity is criminal in jurisdiction X but is not in jurisdiction Y, then the authorities in X could not extradite a criminal in Y.
16. Treaty Office, Directorate of Legal Advice and Public International Law, Council of Europe, "Details of Treaty No. 185: Convention on Cybercrime," https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
17. Cybercrime, Council of Europe, "Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY," https://www.coe.int/en/web/cybercrime/parties-observers.
18. U.S. Clarifying Lawful Overseas Use of Data Act ("CLOUD" Act), 18 U.S. Code §2523, https://www.justice.gov/dag/page/file/1152896/download.
19. LOC (2018).
20. Council of the European Union (2019).
21. EC (2018a).
22. EC (2014).
23. Sources differ on the number of data protection laws enacted around the world: 128 countries, according to the United Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide (dashboard), https://unctad.org/page/data-protection-and-privacy-legislation-worldwide; 116 countries, according to DLA Piper (2020); and 142 countries (as of 2019), according to Greenleaf and Cottier (2020), as referenced by Anderson and Renieris (2020).
24. Consent is not the only basis for data processing, but it remains a centerpiece because of its historical legacy. Even in the GDPR, consent is one among many grounds for legitimate data processing. See, for example, GDPR Article 6.1 (EU 2018a).
25. See Recital 43 of the GDPR (EU 2018c).
26. For example, the US Fair Credit Reporting Act bans certain types of data from being used to determine an individual's creditworthiness (FTC 2018).
27. Section 35 of the Personal Data Protection Bill currently under discussion in India states that, in the event of an imminent threat to the sovereignty or integrity of the country or security of the state, the government has the power to exempt public sector entities from application of the bill entirely (Parliament of India 2019).
28. Sections 13(1) and (2) of India's Personal Data Protection Bill (2018) state that, until and unless such a threat occurs, personal data may be processed without procuring consent from the user in the following cases: "(1) Personal data may be processed if such processing is necessary for any function of Parliament or any State Legislature. (2) Personal data may be processed if such processing is necessary for the exercise of any function of the State authorised by law for: (a) the provision of any service or benefit to the data principal from the State; or (b) the issuance of any certification, license or permit for any action or activity of the data principal by the State" (Personal Data Protection Bill, 2018, https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf).
29. See Article 8 of the European Convention on Human Rights on the right to respect for private and family life (ECHR 2010). The European Court of Human Rights (ECHR) has interpreted limitations to the right as subject to a "legitimate aim" necessary to fulfill a "pressing social need" and "proportionate to the legitimate aim pursued" (ECHR 2020, 12). These due process restrictions apply even in emergency situations—see Article 15 (ECHR 2010). Such situations could include war or pandemic. The European Data Protection Board (EDPB 2018), civil society organizations such as the Electronic Frontier Foundation (see, for example, Gelman 1998), and Article 19 of the European Convention have enshrined these principles into data protection rules and guidelines. See Electronic Frontier Foundation, "13 International Principles on the Application of Human

Rights to Communication Surveillance," https://www.eff.org/files/2014/01/05/13p-onepagerfinal.pdf.

30. Ben-Avie and Tiwari (2019).
31. According to the World Economic Forum, "volunteered data" are data that are "created and explicitly shared by individuals, e.g., social network profiles"; "observed data" are "captured by recording the actions of individuals, e.g., location data when using cell phones"; and "inferred data" are "data about individuals based on an analysis of volunteered or observed information, e.g., credit scores" (WEF 2011).
32. Austin and Lie (2019). See also Recital 26 of the GDPR: "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable" (EU 2018b). Pseudonymized data, however, still count as personally identifiable information.
33. Austin and Lie (2019); de Montjoye et al. (2013). Additional research argues that only three data points are needed for reidentification in most cases (Sweeney 2000). There is also much recent research on the limits and durability of these deidentifying technologies (Lubarsky 2017).
34. Austin and Lie (2019). For example, scientific research may require certain personally identifiable information characteristics (such as age and gender) for accuracy.
35. Current international guidelines for data collection and processing, such as the 2013 OECD guidelines and the United Nations Data Privacy, Ethics and Protection Principles (UNSDG 2017), and leading legal frameworks such as the European Union's General Data Protection Regulation (EU 2018f), focus on protecting personal data and professionally identifiable information. For a broader discussion, see Taylor, Floridi, and van der Sloot (2017).
36. Krämer, Senellart, and de Streel (2020).
37. A purpose-driven approach to data protection should involve determining as threshold questions what data should be collected and what data should be shared. Anonos, "Schrems II Webinar Summary: Lawful Data Transfers," https://www.schremsii.com/faqs-and-summary-edps-noyb-webinar.
38. In other words, focus on the ways in which the data will and may be used and what its potential impacts may be. For this reason, tools such as data protection impact assessments (and, when appropriate, human rights impact assessments, such as when high-risk, data-driven technologies are being used) can help identify risks that must be mitigated through the appropriate legal, technical, and organizational means.
39. Cavoukian (2011).
40. For example, homomorphic encryption allows analysis of encrypted data. Similar in purpose, federated learning techniques allow data to be processed and analyzed without having to send raw data to a central server (Homomorphic Encryption Standardization, "Homomorphic Encryption," https://homomorphicencryption.org/; Potey, Dhote, and Sharma 2016). That said, encryption is not a silver bullet for compliance. Encryption may be an effective safeguard while data are in storage or in transit, but it may not provide sufficient protection for processing if data must be de-encrypted before computation.
41. Newer techniques that have emerged in response to challenges around deidentification include K-anonymity (works by aggregating data attributes) and differential privacy (works by introducing random noise into datasets)—see Austin and Lie (2019); Dwork (2006); Sweeney (2000).
42. The European Commission's guidance on privacy by design is clear that these techniques should not be a substitute for robust legal protections: "The term 'Privacy by Design' means nothing more than 'data protection through technology design.' Behind this is the thought that data protection in data processing procedures is best adhered to when it is already integrated in the technology when created. . . . The text of the law leads one to conclude that often several protective measures must be used with one another to satisfy statutory requirements. In practice, this consideration is already performed in an early development phase when setting technology decisions. Recognized certification can serve as an indicator to authorities that the persons responsible have complied with the statutory requirements of 'Privacy by Design'" (Intersoft Consulting, "GDPR: Privacy by Design," https://gdpr-info.eu/issues/privacy-by-design/). Also see DSGVO-Portal, "Recital 78 GDPR | General Data Protection Regulation," https://www.dsgvo-portal.de/gdpr_recital_78.php.
43. The Mauritius Declaration on the Internet of Things states: "Data processing starts from the moment the data are collected. All protective measures should be in place from the outset. We encourage the development of technologies that facilitate new ways to incorporate data protection and consumer privacy from the outset. Privacy by design and default should no longer be regarded as something peculiar. They should become a key selling point of innovative technologies" (EDPS 2014, 2).
44. The International Organization for Standardization has created a technical committee for a new ISO standard on Consumer Protection: Privacy by Design for Consumer Goods and Services (ISO 2018).
45. Cavoukian (2010).
46. According to the European Commission: "Companies/organisations are encouraged to implement technical and organisational measures, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles right from the start ('data protection by design'). By default, companies/organisations should ensure that personal data is processed with the highest privacy protection (for example only the data necessary should be processed, short storage period, limited accessibility) so that by default personal data isn't made accessible to an indefinite number of persons ('data protection

by default')." European Commission, "What Does Data Protection 'by Design' and 'by Default' Mean?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en.

47. OVIC (2020).
48. See PCPD (2012) for materials on the data protection framework in China.
49. ICO (2018).
50. de Montjoye at al. (2013). Additional research argues that only three data points are needed for reidentification in most cases (Sweeney 2000).
51. These new techniques include statistical approaches such as K-anonymity, which aggregates data attributes (Sweeney 2002); differential privacy, which introduces random noise (Dwork 2006); and encryption techniques such as homomorphic encryption, which conduct analysis on encrypted data (Potey, Dhote, and Sharma 2016).
52. Austin and Lie (2019).
53. See Hasselbalch and Tranberg (2016). An explanation of a personal data store is offered in Mydex, "What Is a Personal Data Store?" https://pds.mydex.org/what-personal-data-store-0.
54. ENISA (2014). Also see the recommendation by the European Union Agency for Cybersecurity (ENISA) that it may be necessary to overlay several privacy by design or pseudonymization techniques in order to meet the GDPR's threshold (ENISA 2019).
55. The OECD Recommendation on Artificial Intelligence "identifies five complementary values-based principles for the responsible stewardship of trustworthy AI" (OECD 2019c). In particular, according to principle 2 on human-centered values and fairness, "AI actors should respect the rule of law, human rights, and democratic values throughout the AI system life cycle. These include freedom, dignity and autonomy, privacy and data protection, nondiscrimination and equality, diversity, fairness, social justice, and internationally recognized labor rights." These actors should also "implement mechanisms and safeguards, such as capacity for human determination, that are appropriate to the context." According to principle 3 on transparency and explainability, "AI actors should commit to transparency and responsible disclosure regarding AI systems." One of the aims should be "to enable those adversely affected by an AI system to challenge [the] outcome based on plain and easy-to-understand information." As of May 2019, 44 countries had adhered to the OECD Recommendation and the five principles (OECD 2019c).
56. See Loi N° 2013-450 relative à la protection des données à caractère personnel [Law 2013-450 on the protection of personal data], *Journal Officiel de la Republique de Côte d'Ivoire*, August 8, 2013, 474–82.
57. Controversies around the use of facial recognition and other AI-based technologies for law enforcement have been in the public eye in the United Kingdom since 2019, when the UK Information Commissioner Office launched an investigation into the use of facial recognition technology in King's Cross in London, on the grounds that it might raise data protection concerns. Subsequently, the UK High Court's decision in favor of the use of facial recognition by the South Wales Police, after the claimant argued that its use would be a violation of privacy, was the first legal challenge to the use of facial recognition by police in the world. See ICO (2019); Nilsson (2019); Smith (2016).
58. The 2016 study conducted by the Human Rights Data Analysis Group using 2010 and 2011 data from the Oakland police department and other sources compared a mapping of drug use based on survey data from the victims of crime with another based on algorithmic analysis of police arrests. The study showed that biased source data could reinforce and potentially amplify racial bias in law enforcement practices (Lum 2016). Data on arrests showed that African-American neighborhoods have on average 200 times more drug arrests than other areas in Oakland (NIST 2020; Smith 2016).
59. Hill (2020).
60. Noble (2018).
61. Dastin (2018).
62. Organisation for Economic Co-operation and Development, http://www.oecd.org/going-digital/ai/principles/; G-20 (Japan-led), https://www.meti.go.jp/press/2019/06/20190610010/20190610010-1.pdf.
63. HLCM (2018).
64. Cision (2020); City of Amsterdam (2020); City of Helsinki (2020).
65. DCMS (2019); Stats NZ (2019). For a subnational example, see Nantes City's Metropolitan Charter on Data (Ville de Nantes 2019). At a national level, France's Etalab has developed a map of algorithmic systems in use across public sector entities in France and is providing ministries, departments, and agencies with guidance on their reporting and other accountability requirements (Etalab 2020a, 2020b).
66. See Canada's responsible use of AI in government programs, including Guiding Principles, lists of certified providers of AI services, and its Algorithmic Impact Assessment (TBS 2020).
67. Henley and Booth (2020).
68. The mandate of the US Federal Trade Commission (FTC) includes hearing and adjudicating cases involving unfair competition or unfair or deceptive acts under Section 5 of the FTC Act (see Federal Trade Commission, Federal Trade Commission Act, https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act). According to the FTC, "when companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up [to] these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair

and deceptive acts and practices in or affecting commerce. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security" (see Federal Trade Commission, "Privacy and Security Enforcement," https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement).

69. Hoofnagle, Hartzog, and Solove (2019).
70. In the context of its 2020 European Data Strategy, the EU may adopt a new Data Act in 2021, which would update the IPR framework currently in force (including a possible revision of the 1996 Database Directive) to support the use and reuse of nonpersonal data (EC 2020b).
71. See, for example, Contract Guidelines on Data Utilization Rights, updating the Unfair Competitive Prevention Act of 2018 (METI 2020).
72. MeitY (2020).
73. See World Intellectual Property Organization, "Brazil: Law No. 9.610 of February 19, 1998 (Law on Copyright and Neighboring Rights, as amended by Law No. 12.853 of August 14, 2013)," WIPO Lex (database), https://wipolex.wipo.int/en/legislation/details/17474.
74. See, generally, the two model laws promulgated by the United Nations Commission on International Trade Law (UNCITRAL 1998, 2001).
75. For purposes of this discussion, no distinction is drawn between "electronic" signatures and "digital" signatures, although commonly "digital" signatures are associated with the use of public key infrastructure (PKI). For a more detailed explanation of PKI and the differences between e-signatures and digital signatures, see UNCITRAL (2001, 26–27; https://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf).
76. UNCITRAL (1998).
77. Public key infrastructure (PKI) has been defined as follows: "The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates" (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf).
78. EU (2014, article 3[15]).
79. See, generally, World Bank, ID4D Data: Global Identification Challenge by the Numbers (dashboard), https://id4d.worldbank.org/global-dataset; Sustainable Development, Department of Economic and Social Affairs, United Nations, "The 17 Goals," https://sdgs.un.org/goals. Sustainable Development Goal (SDG) 16.9 states: "By 2030, provide legal identity for all, including birth registration."
80. World Bank (2019).
81. UNCITRAL (1998).
82. National Assembly, Togo (2020).
83. EC (2018c).
84. The Australian government's Data Sharing and Release Act of 2018 was drafted based on the results of a report of the Productivity Commission (PC 2017). The purpose of the act is to (1) promote better sharing of public sector data, (2) build trust in use of public data, (3) dial up or down appropriate safeguards, (4) maintain the integrity of the data system, and (5) establish institutional arrangements (see Department of the Prime Minister and Cabinet, "Data Sharing and Release Reforms," https://www.pmc.gov.au/public-data/data-sharing-and-release-reforms). This is expected to lead to (1) more efficient and effective government services for citizens; (2) more well-informed government programs and policies; (3) greater transparency around government activities and spending; (4) economic growth from innovative data use; and (5) research solutions to current and emerging social, environmental, and economic issues. The purpose of the act is thus to move the paradigm from one that restricts access to identifiable data to one that authorizes release if appropriate data safeguards are in place. To complement the Data Sharing and Release Act, the government published a best-practice guide outlining good-practice principles based on the Five Safes Framework to manage the risks of disclosure and designed to assess whether and how to share data (PMC 2019). By enabling a privacy by design approach to data sharing by focusing on controls and benefits instead of merely reducing the level of detail in the data to be shared, the principles help maximize the usefulness of the data.
85. National Archives (2019).
86. Section 1 of France's Law for a Digital Republic lays out provisions on open government data (Légifrance 2016). Also see Dodds (2016).
87. They include geospatial, meteorological, and mobility data, as well as statistics and data on corporate ownership and Earth observation and the environment.
88. Noveck (2017).
89. Noveck (2017).
90. See Open Knowledge Foundation (2020).
91. OECD (2013, 2019a); Ubaldi (2013); Vickery (2012).
92. Dodds (2016).
93. OECD (2019a).
94. Austin and Lie (2019); Dodds (2016).
95. World Wide Web Foundation (2017).
96. For general principles, see ISO and IEC (2016, sec. 8.2). For a practical example, see Data.NSW (2020).
97. OECD (2019a).
98. OECD (2019a).
99. Austin and Lie (2019).
100. Wilkinson et al. (2016).
101. See Article 3: "Art. L. 300-4.- Any provision made electronically under this book is done in an open standard, easily reusable and exploitable by an automated processing system" of the French Republic (Légifrance 2016).
102. Because the development of open standards is often undertaken with input from leading industry participants, who frequently integrate their firms'

proprietary technical standards into the design, SSOs may require the application of patent rights on FRAND terms. The adoption of FRAND licensing terms can therefore become a condition for participation in SSOs. The obligation to offer FRAND licenses to new market entrants usually extends to third-party technology providers whether or not they are SSO members. For further details, see Ragavan, Murphy, and Davé (2016).

103. The Open Knowledge Foundation's definition of open data ("Open Definition") sets out conditions for the availability and access of data, its reuse and redistribution, and universal participation. On the latter, "everyone must be able to use, re-use and redistribute—there should be no discrimination against fields of endeavor or against persons or groups. For example, 'non-commercial' restrictions that would prevent 'commercial' use, or restrictions of use for certain purposes (e.g. only in education), are not allowed." See Open Knowledge Foundation (2020; https://okfn.org/opendata/).
104. MITCI (2017).
105. Council of Ministers, Jordan (2019).
106. ISO and IEC (2017).
107. EDRi (2015). Ensuring sufficient resources and technical capacity to effectively discharge these functions is critical. For example, Estonia's X-Tee data exchange and interoperability platform is continuously monitored to mitigate cyberthreats (RIA 2020). See chapter 8 for further details on implementation.
108. EC (2016).
109. As the European Commission notes: "Online public services are crucial to increasing the cost-efficiency and quality of the services provided to citizens and companies. One example of increased efficiency is the 'Once Only' principle—only in 48% of cases do public administrations reuse information about the citizen or companies that is already in their possession without asking again. The extension of this principle, in compliance with data protection legislation, would generate an annual net saving at the EU level of around EUR 5 billion per year by 2017. The Commission will launch a pilot project for the 'Once-Only' principle for businesses and citizens and explore the possibility of an EU wide e-safe solution (a secure online repository for documents). Extending 'Once-Only' across borders would further contribute to the efficiency of the Digital Single Market" (EC 2015, 16).
110. TOOP (2021).
111. See European Commission, "Horizon 2020," https://ec.europa.eu/programmes/horizon2020/en.
112. SCOOP4C, "Stakeholder Community: Once-Only Principle for Citizens," https://www.scoop4c.eu/.
113. OECD (2019a).
114. OECD (2019a).
115. EU (2019b).
116. EC (2020a).
117. Légifrance (2016). This covers, for example, data from delegated public services or data that are relevant for targeting welfare payments or constructing national statistics (OECD 2019a).
118. The UK Digital Economy Act enables accredited researchers to gain access to deidentified data for research purposes (National Archives, United Kingdom 2017, c. 30, Chap. 5). The act regulates data sharing practices for the purposes of research using public data, but it does not govern data sharing in other contexts (Austin and Lie 2019).
119. Finch and Tene (2018).
120. OECD (2019b).
121. Ragavan, Murphy, and Davé (2016).
122. FRAND licensing regimes have been designed to be an effective competition law remedy (see the *Apple vs. Samsung* cases), but infringements of FRAND terms involve contractual remedies between the patent holder and the SSO (or third party). However, experts have argued that the pro-innovation and competitive effects of licensing regimes depend on how they are implemented. Indeed, some have argued that an "excessive reliance" on FRAND terms may be counterproductive.
123. Open Knowledge Foundation, "Open Data Commons Open Database License (ODbL) v1.0," https://opendatacommons.org/licenses/odbl/1-0/.
124. Creative Commons, "Open Data," https://creativecommons.org/about/program-areas/open-data/.
125. MoICT (2017).
126. See the European Union's Free Flow of Nonpersonal Data Regulation (EU 2018e), the Payment Services Directive (EU 2015), the Digital Content Directive (EU 2019a), and certain sectoral regulations, in addition to the right to data portability for personal data enshrined in Article 20 of the GDPR. See also Borgogno and Colangelo (2019).
127. Article 20 of the GDPR (EU 2016).
128. The European Commission notes: "In general, given the policy objectives of the right to data portability, the term 'provided by the data subject' must be interpreted broadly, and should exclude 'inferred data' and 'derived data,' which include personal data that are created by a service provider (for example, algorithmic results). A data controller can exclude those inferred data but should include all other personal data provided by the data subject through technical means provided by the controller" (EC 2017). This approach contrasts with that of other legal frameworks, such as the California Consumer Protection Act (CCPA), that are broader in scope covering inferred data (see OneTrust DataGuidance and FPF 2019).
129. Krämer, Senellart, and de Streel (2020).
130. See Recital 68 of the GDPR: "Data controllers should be encouraged to develop interoperable formats that enable data portability. . . . The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. . . . Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another" (EU 2018d).

131. See Article 6, "Porting of Data," of the EU Regulation on the Free Flow of Non-personal Data: "The Commission shall *encourage and facilitate* [emphasis added] the development of self-regulatory codes of conduct at Union level ('codes of conduct'), in order to contribute to a competitive data economy" (EU 2018e, 67).
132. PIMS can help individuals control their ported data through mechanisms that simplify the process. They can include mechanisms that support individual control over ported data such as schema mappings (which convert data from the sender's format to the receiver's) or functionalities that centralize and help visualize consent and rights management for portability or broader data protection. However, these mechanisms have not been standardized across the industry to date, which affects the broader sustainability of the business model and their adoption as an alternative to other enforcement mechanisms.
133. Measures such as shifting to authentication mechanisms (like privacy seals) and open-source solutions that are more user friendly may support the adoption of PIMS as alternatives for consumers, especially if the reliability of these solutions are certified to promote trust (Krämer, Senellart, and de Streel 2020).
134. The first right to portability mandated by EU law was the portability of phone numbers, following the Universal Services Directive, based on a legislative effort to create competition in the telecommunications sector (Zanfir-Fortuna and Hondagneu-Messner 2019).
135. Borgogno and Colangelo (2019).
136. Congress of the Philippines (2012).
137. The "consumer data right" aims to "give Australians greater control over their data, empowering their consumers to choose to share their data with trusted recipients only for the purposes they have authorized" (Treasury, Australia 2020).
138. See Part IVD in Federal Register of Legislation, Australia (2019).
139. The act begins with the telecommunications, banking, and energy sectors before rolling out across the economy.
140. The data standards body has released version 1.6.0 of the consumer data standards, which represent high-level standards and are in accordance with the rules and phasing timetable of the Australian Competition and Consumer Commission. See Data61, Commonwealth Scientific and Industrial Research Organisation, "Consumer Data Standards," https://consumerdatastandards.gov.au/consumer-data-standards/.
141. At present, the Data Transfer Project is at the pilot stage, making it difficult to measure the impact of the project on enabling continuous portability of data. It remains an interesting model of private sector–led cooperation to develop standard and interoperable data formats that could be scaled up. See Google, "Data Transfer Project," https://datatransferproject.dev/. The founding members of the Data Transfer Project were Google and Facebook. They were later joined by Apple, Microsoft, and Twitter.
142. Borgogno and Colangelo (2019).
143. OECD (2019a).
144. This was a point of discussion at the international policy workshop "Data for Better Lives: Enablers and Safeguards" hosted by the World Bank and the German Federal Ministry of Economic Cooperation and Development in Washington, DC, June 9–10, 2020.
145. See Berlin Group, "PSD2 Access to Bank Accounts," https://www.berlin-group.org/psd2-access-to-bank-accounts.
146. Waze (2018).
147. Google, "Waze for Cities: Working Together for a Smarter, More Sustainable Future," *Waze*, https://www.waze.com/ccp. Waze and other companies have been sharing data with local governments in Brazil since the 2016 Rio Olympics under their Connected Citizens Program. Their platform is designed to support public entities with urban planning, traffic optimization, law enforcement, and emergency service provision (Huyer and Cecconi 2020).
148. OECD (2019a).
149. Huyer and Cecconi (2020).
150. These include Japan's "Contract Guidance on Utilization of AI and Data" (METI 2018); the Netherlands' Dare-2-Share Cooperation Agreement (Dare 2 Share Ministries, "Terms and Conditions," https://www.dare2share.org/about/terms-and-conditions/); and the European Union's proposed "Guidance on Private Sector Data Sharing" (EC 2018b). Japan's Ministry of Economy, Trade and Industry (METI) developed the "Contract Guidance on Utilization of AI and Data" as a resource for businesses entering a data sharing agreement. It highlights factors and terms to be considered for inclusion when drafting a contract using data or AI, including sample clauses.
151. Kirkpatrick (2014).
152. See "Development Data Partnership," https://datapartnership.org/.
153. GPO (2018).
154. Kosseff (2019, 27).
155. GPO (2018, at sec. 230).
156. LOC (1998).
157. Kosseff (2019, 5).
158. See Electronic Frontier Foundation, "Manila Principles on Intermediary Liability," https://www.manilaprinciples.org/.

References

Anderson, Thea, and Elizabeth M. Renieris. 2020. "Data Protection and Digital Infrastructure before, during, and after a Pandemic." Omidyar Network, Redwood City, CA. https://omidyar.com/data-protection-and-digital-infrastructure-before-during-and-after-a-pandemic/.

Austin, Lisa M., and David Lie. 2019. "Safe Sharing Sites." *NYU Law Review* 94 (4): 591–623. https://www.nyulawreview.org/issues/volume-94-number-4/safe-sharing-sites/.

Ben-Avie, Jochai, and Udbhav Tiwari. 2019. "India's New Data Protection Bill: Strong on Companies, Step Backward

on Government Surveillance." *Open Policy and Advocacy* (blog), December 10, 2019. https://blog.mozilla.org/netpolicy/2019/12/10/indias-new-data-protection-bill-strong-on-companies-weak-on-gov.

Borgogno, Oscar, and Giuseppe Colangelo. 2019. "Data Sharing and Interoperability: Fostering Innovation and Competition through APIs." *Computer Law and Security Review* 35 (5): 105314. https://doi.org/10.1016/j.clsr.2019.03.008.

Cavoukian, Ann. 2010. "Privacy by Design: The Definitive Workshop; A Foreword by Ann Cavoukian, Ph.D." *Identity in the Information Society* 3 (2): 247–51. https://doi.org/10.1007/s12394-010-0062-y.

Cavoukian, Ann. 2011. "PbD, Privacy by Design, the 7 Foundational Principles: Implementation and Mapping of Fair Information Practices." Information and Privacy Commissioner of Ontario, Toronto.

Chen, Rong. 2021. "Mapping Data Governance Legal Frameworks around the World: Findings from the Global Data Regulation Diagnostic." Policy Research Working Paper 9615, World Bank, Washington, DC. http://documents.worldbank.org/curated/en/581331617817680243/Mapping-Data-Governance-Legal-Frameworks-Around-the-World-Findings-from-the-Global-Data-Regulation-Diagnostic.

Cision. 2020. "Helsinki and Amsterdam First Cities in the World to Launch Open AI Register." *Cision News*, September 28, 2020. Cision, Chicago. https://news.cision.com/fi/city-of-helsinki/r/helsinki-and-amsterdam-first-cities-in-the-world-to-launch-open-ai-register,c3204076.

City of Amsterdam. 2020. "What Is the Algorithm Register?" *City of Amsterdam Algorithm Register Beta*. https://algoritmeregister.amsterdam.nl/en/ai-register/.

City of Helsinki. 2020. "What Is an Artificial Intelligence Register?" *City of Helsinki Artificial Intelligence Register*. https://ai.hel.fi/.

COE (Council of Europe). 2018. "Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data." COE, Strasbourg. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

Confessore, Nicholas. 2018. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." *New York Times*, April 4, 2018. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Congress of the Philippines. 2012. "Republic Act No. 10173: An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes." August 12, 2012, Lawphil Project, Arellano Law Foundation, Manila. https://lawphil.net/statutes/repacts/ra2012/ra_10173_2012.html.

Council of Ministers, Jordan. 2019. "Jordan Open Government Data License." Issue version 1.0, Open Government Data Platform. https://portal.jordan.gov.jo/OGD-License_en.pdf.

Council of the European Union. 2019. "Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters." Interinstitutional File 2018/0108(COD), Council of the European Union, Brussels. https://data.consilium.europa.eu/doc/document/ST-10206-2019-INIT/en/pdf.

Dastin, Jeffrey. 2018. "Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women." *Reuters*, October 10, 2018. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

Data.NSW. 2020. "NSW Government Information Classification, Labelling, and Handling Guidelines." Data.NSW, Data Analytics Center, Customer, Delivery, and Transformation, Department of Customer Service, Government of New South Wales, Sydney. https://www.digital.nsw.gov.au/sites/default/files/NSW%20Info%20Classification%20Labelling%20and%20Handling%20Guidelines%202020%20V2.1_1.pdf.

DCMS (Department for Digital, Culture, Media, and Sport, United Kingdom). 2019. "Digital Charter." Policy Paper, DCMS, London. https://www.gov.uk/government/publications/digital-charter/digital-charter.

Deighton-Smith, Rex, Angelo Erbacci, and Céline Kauffmann. 2016. "Promoting Inclusive Growth through Better Regulation: The Role of Regulatory Impact Assessment." OECD Regulatory Policy Working Paper 3, Organisation for Economic Co-operation and Development, Paris. https://doi.org/10.1787/5jm3tqwqp1vj-en.

de Montjoye, Yves-Alexandre, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel. 2013. "Unique in the Crowd: The Privacy Bounds of Human Mobility." *Scientific Reports* 3 (1): article 1376. https://doi.org/10.1038/srep01376.

DLA Piper. 2020. *Data Protection Laws of the World*. London: DLA Piper. https://www.dlapiperdataprotection.com/index.html?t=about&c=AO.

Dodds, Leigh. 2016. "How to Write a Good Open Data Policy." *Guides*. Open Data Institute, London.

Dong, Marissa Xiao. 2020. "China: The Civil Code Strengthens Civil Law Protection around Privacy and Personal Information." *Conventus Law*, June 12, 2020. http://www.conventuslaw.com/report/china-the-civil-code-strengthens-civil-law/.

Dwork, Cynthia. 2006. "Differential Privacy." In *Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10–14, 2006, Proceedings, Part II*, edited by Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, 1–12. Lecture Notes in Computer Science Series, Vol. 4052. Berlin: Springer. https://link.springer.com/chapter/10.1007%2F11787006_1.

EC (European Commission). 2014. "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on 'Google Spain and INC v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12." Document WP225, Directorate C (Fundamental Rights and Union Citizenship), Directorate General Justice, EC, Brussels. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=667236.

EC (European Commission). 2015. "A Digital Single Market Strategy for Europe." Document COM(2015) 192 final, EC, Brussels. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN.

EC (European Commission). 2016. "EU eGovernment Action Plan 2016–2020: Accelerating the Digital Transformation

of Government." Document COM(2016) 179 final, EC, Brussels. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0179.

EC (European Commission). 2017. "Article 29 Data Protection Working Party: Guidelines on the Right to Data Portability." Document WP242 rev.01, Directorate C (Fundamental Rights and Rule of Law), Directorate General Justice and Consumers, EC, Brussels. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

EC (European Commission). 2018a. "Article 29 Working Party: Guidelines on Consent under Regulation 2016/679." Document WP259 rev.01, Directorate C (Fundamental Rights and Union Citizenship), Directorate General Justice, EC, Brussels. https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030.

EC (European Commission). 2018b. "Guidance on Private Sector Data Sharing." Text. Shaping Europe's Digital Future—European Commission. https://ec.europa.eu/digital-single-market/en/guidance-private-sector-data-sharing.

EC (European Commission). 2018c. *Study to Support the Review of Directive 2003/98/EC on the Re-Use of Public Sector Information: Final Report*. Luxembourg: Publications Office of the European Union. https://data.europa.eu/doi/10.2759/373622.

EC (European Commission). 2020a. "European Legislation on Open Data and the Re-Use of Public Sector Information." *Shaping Europe's Digital Future: Policy*. Data Policy and Innovation (Unit G.1), EC, Brussels. https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information.

EC (European Commission). 2020b. "A European Strategy for Data." Communication COM(2020) 66 final, Brussels, EC. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

ECHR (European Court of Human Rights). 2010. "European Convention on Human Rights." ECHR and Council of Europe, Strasbourg. https://www.echr.coe.int/documents/convention_eng.pdf.

ECHR (European Court of Human Rights). 2020. *Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence*, rev. ed. Strasbourg: ECHR. https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

EDPB (European Data Protection Board). 2018. "Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679." *Guidelines*. EDPB, Brussels. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

EDPS (European Data Protection Supervisor). 2014. "Mauritius Declaration on the Internet of Things." 36th International Conference of Data Protection and Privacy Commissioners, Balaclava, Mauritius, October 14, 2014. https://edps.europa.eu/sites/edp/files/publication/14-10-14_mauritius_declaration_en.pdf.

EDRi (European Digital Rights). 2015. "A Truly Digital Single Market?" June, EDRi, Brussels. https://edri.org/files/DSM_Analysis_EDRi_20150617.pdf.

ENISA (European Union Agency for Cybersecurity). 2014. "Privacy and Data Protection by Design: From Policy to Engineering." ENISA, Heraklion, Greece. https://data.europa.eu/doi/10.2824/38623.

ENISA (European Union Agency for Cybersecurity). 2019. "Pseudonymisation Techniques and Best Practices: Recommendations on Shaping Technology According to Data Protection and Privacy Provisions." ENISA, Heraklion, Greece. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.

Etalab. 2020a. "Algorithmes de Nantes Métropole." *data.gouv.fr*, October 7, 2020, Etalab, Paris. https://www.data.gouv.fr/en/datasets/algorithmes-de-nantes-metropole/.

Etalab. 2020b. "Les algorithmes publics: enjeux et obligations" [Public sector algorithms: challenges and obligations]. *guides.etalab.gouv.fr*, Etalab, Paris. https://guides.etalab.gouv.fr/algorithmes/guide/#_1-a-quoi-servent-les-algorithmes-publics.

EU (European Union). 2014. "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC." *Official Journal of the European Union* L 257/73 (August 8). https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf.

EU (European Union). 2015. "Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC." *Official Journal of the European Union* L 337/35 (December 23). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN.

EU (European Union). 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)." *Official Journal of the European Union* L 119/1 (May 4). https://eur-lex.europa.eu/eli/reg/2016/679/oj.

EU (European Union). 2018a. "Art. 6 GDPR: Lawfulness of Processing." *GDPR.Eu*, November 14, 2018. Proton Technologies, Calgary, Canada. https://gdpr.eu/article-6-how-to-process-personal-data-legally/.

EU (European Union). 2018b. "Recital 26: Not Applicable to Anonymous Data." *GDPR.Eu*, November 14, 2018. Proton Technologies, Calgary, Canada. https://gdpr.eu/recital-26-not-applicable-to-anonymous-data/.

EU (European Union). 2018c. "Recital 43: Freely Given Consent." *GDPR.Eu*, November 14, 2018. Proton Technologies, Calgary, Canada. https://gdpr.eu/recital-43-freely-given-consent/.

EU (European Union). 2018d. "Recital 68: Right of Data Portability." *GDPR.Eu*, November 14, 2018. Proton Technologies, Calgary, Canada. https://gdpr.eu/recital-68-right-of-data-portability/.

EU (European Union). 2018e. "Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-personal Data in the European Union." *Official Journal of the European Union* L 303, 61 (November 10): 78–68. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2018:303:FULL&from=EN.

EU (European Union). 2018f. "What Is GDPR, the EU's New Data Protection Law?" *GDPR.Eu*, May 25, 2018. Proton Technologies, Calgary, Canada. https://gdpr.eu/what-is-gdpr/.

EU (European Union). 2019a. "Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services." *Official Journal of the European Union* L 136/1 (May 22). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0770&from=EN.

EU (European Union). 2019b. "Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the Re-Use of Public Sector Information." *Official Journal of the European Union* L 172/56 (June 26). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024&from=EN.

Fang, Sammy, Carolyn Bigg, and John Zhang. 2020. "New Chinese Civil Code Introduces Greater Protection of Privacy Rights and Personal Information." *Insights*, June 9, 2020, DLA Piper, London. https://www.dlapiper.com/en/uk/insights/publications/2020/06/new-chinese-civil-code-introduces-greater-protection-of-privacy-rights-and-personal-information/.

Federal Register of Legislation, Australia. 2019. "Competition and Consumer Act 2010, No. 51, 1974." *Compilation* 121. Sydney: Office of Parliamentary Counsel. http://www.legislation.gov.au/Details/C2019C00317/Html/Volume_1.

Finch, Kelsey, and Omer Tene. 2018. "Smart Cities: Privacy, Transparency, and Community." In *The Cambridge Handbook of Consumer Privacy*, edited by Evan Selinger, Jules Polonetsky, and Omer Tene, 125–48. Cambridge Law Handbooks Series. Cambridge, UK: Cambridge University Press. https://doi.org/10.1017/9781316831960.007.

Fisher, Angelina, and Thomas Streinz. 2021. "Confronting Data Inequality." WDR 2021 background paper, World Bank, Washington, DC. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3825724.

FTC (Federal Trade Commission, United States). 2018. *Fair Credit Reporting Act, 15 U.S.C § 1681*, rev. ed. Washington, DC: FTC. https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf.

Gellman, Barton. 2013. "Edward Snowden, after Months of NSA Revelations, Says His Mission's Accomplished." *Washington Post*, December 23, 2013. https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html.

Gelman, Robert B. 1998. *Protecting Yourself Online: The Definitive Resource on Safety, Freedom, and Privacy in Cyberspace*. With Stanton McCandlish and Members of the Electronic Frontier Foundation. New York: HarperCollins.

GPO (Government Publishing Office, United States). 2018. *Communications Act of 1934, as Amended*. United States Code, 2018 ed. Title 47: *Telecommunications*. Washington, DC: GPO. https://www.govinfo.gov/app/details/USCODE-2018-title47/USCODE-2018-title47-chap5-subchapI-sec151.

Greenleaf, Graham, and Bertil Cottier. 2020. "2020 Ends a Decade of 62 New Data Privacy Laws." *Privacy Laws and Business International Report* 163: 24–26. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611.

Hasselbalch, Gry, and Pernille Tranberg. 2016. "Personal Data Stores Want to Give Individuals Power over Their Data." *Dataethics* (blog), September 27, 2016. https://dataethics.eu/personal-data-stores-will-give-individual-power-their-data/.

Henley, Jon, and Robert Booth. 2020. "Welfare Surveillance System Violates Human Rights, Dutch Court Rules." *Guardian*, February 5, 2020. https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules.

Hill, Kashmir. 2020. "Wrongfully Accused by an Algorithm." *New York Times*, August 3, 2020. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

HLCM (High-Level Committee on Management, United Nations). 2018. "Personal Data Protection and Privacy Principles." HLCM, Chief Executives Board for Coordination, United Nations, Geneva. https://unsceb.org/personal-data-protection-and-privacy-principles.

Hoofnagle, Chris Jay, Woodrow Hartzog, and Daniel J. Solove. 2019. "The FTC Can Rise to the Privacy Challenge, but Not without Help from Congress." *Brookings TechTank* (blog), August 8, 2019. https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/.

Huyer, Esther, and Gianfranco Cecconi. 2020. "Business-to-Government Data Sharing." Analytical Report 12, European Data Portal, European Commission, Luxembourg. https://www.europeandataportal.eu/sites/default/files/analytical_report_12_business_government_data_sharing.pdf.

ICO (Information Commissioner's Office). 2018. *Guide to the General Data Protection Regulation (GDPR)*. Wilmslow, UK: ICO. https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf.

ICO (Information Commissioner's Office). 2019. "The Use of Live Facial Recognition Technology by Law Enforcement in Public Places." *Information Commissioner's Opinion*, 2019/01, October 31, 2019. https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

ISO (International Organization for Standardization). 2018. "ISO/PC 317: Consumer Protection: Privacy by Design for Consumer Goods and Services." *Taking Part: Technical Committee*, ISO, Geneva. https://www.iso.org/committee/6935430.html.

ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). 2016. "ISO/IEC 27011:2016(en): Information Technology, Security Techniques, Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Telecommunications Organizations." Online Browsing Platform, ISO, Geneva, https://www.iso.org/obp/ui/#iso:std:iso-iec:27011:ed-2:v1:en.

ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). 2017. "ISO/IEC 19941:2017, Information Technology, Cloud Computing, Interoperability, and Portability." Online

Browsing Platform, ISO, Geneva. https://www.iso.org/obp/ui/#iso:std:iso-iec:19941:ed-1:v1:en.

ITU (International Telecommunication Union). 2014. "Using Regulatory Impact Analysis to Improve Decision Making in the ICT Sector." ITU, Geneva.

Kirkpatrick, Robert. 2014. "A Big Data Revolution for Sustainable Development." In *The Global Compact International Yearbook 2014*, edited by United Nations Global Compact Office, 33–35. New York: United Nations; Münster, Germany: macondo publishing.

Kosseff, Jeff. 2019. *The Twenty-Six Words That Created the Internet*. Ithaca, NY: Cornell University Press.

Krämer, Jan, Pierre Senellart, and Alexandre de Streel. 2020. "Making Data Portability More Effective for the Digital Economy: Economic Implications and Regulatory Challenges." Center on Regulation in Europe, Brussels. https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/.

Légifrance. 2016. "Loi no 2016-1321 du 7 octobre 2016 pour une République numérique." *Journal officiel de la République française*, October 8, 2016, Légifrance, Direction de l'information légale et administrative, Paris. https://www.legifrance.gouv.fr/download/file/SJ9w29KN2wvvWjcmiPwHr3BoLa5rYk6ys5dm_FwTPZs=/JOE_TEXTE.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.

LOC (Library of Congress, United States). 1998. "H. R. 2281 Digital Millennium Copyright Act: 105th Congress (1997–1998)." *Congress.gov*, October 28, 1998, LOC, Washington, DC. https://www.congress.gov/bill/105th-congress/house-bill/2281.

LOC (Library of Congress, United States). 2018. "H. R. 4943, CLOUD Act: 115th Congress (2017–2018)." *Congress.gov*, February 6, 2018, LOC, Washington, DC. https://www.congress.gov/bill/115th-congress/house-bill/4943.

Lubarsky, Boris. 2017. "Re-Identification of 'Anonymized' Data." *Georgetown Law Technology Review* (April): 202–13. https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/.

Lum, Kristian. 2016. "Predictive Policing Reinforces Police Bias." *HRDAG: Human Rights Data Analysis Group*, October 10. http://hrdag.org/2016/10/10/predictive-policing-reinforces-police-bias/.

MeitY (Ministry of Electronics and Information Technology). 2020. "Report by the Committee of Experts on Non-Personal Data Governance Framework." 111972/2020/CL & ES. MeitY, New Delhi. https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/08/mygov_159453381955063671.pdf.

METI (Ministry of Economy, Trade, and Industry, Japan). 2018. "METI Formulates 'Contract Guidance on Utilization of AI and Data.'" News release, June 15, 2018. https://www.meti.go.jp/english/press/2018/0615_002.html.

METI (Ministry of Economy, Trade, and Industry, Japan). 2020. "Unfair Competition Prevention Act." *Policy Index*. Intellectual Property Policy Office, METI, Tokyo. https://www.meti.go.jp/english/policy/economy/chizai/chiteki/index.html.

MITCI (Ministry of Technology, Communication, and Innovation, Mauritius). 2017. "National Open Data Policy." MITCI, Quatre Bornes, Mauritius. https://mitci.govmu.org/Documents/Strategies/Mauritius%20Open%20Data%20Policy%20May%202017.pdf.

MoICT (Ministry of Information and Communication Technology, Jordan). 2017. "Open Government Data Policy." MoICT, Amman, Jordan. https://modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/open_government_data_policy_2017.pdf.

National Archives, United Kingdom. 2017. "Digital Economy Act 2017." *legislation.gov.uk*, National Archives, London. https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted.

National Archives, United Kingdom. 2019. "Guidance on the Implementation of the Re-use of Public Sector Information Regulations 2015: For Public Sector Bodies." Version 1.1, National Archives, London. https://www.nationalarchives.gov.uk/documents/information-management/psi-implementation-guidance-public-sector-bodies.pdf.

National Assembly, Togo. 2020. "Loi Relative a l'Identification Biometrique des Personnes Physiques au Togo" [Law on the biometric measurement of natural persons in Togo]. National Assembly, Open Session, September 3. http://www.assemblee-nationale.tg/images/biometrie%20loi%20AN.pdf.

Nilsson, Patricia. 2019. "Police Fear Bias in Use of Artificial Intelligence to Fight Crime." *Financial Times*, September 15, 2019. https://www.ft.com/content/5753689c-d63e-11e9-a0bd-ab8ec6435630.

NIST (National Institute of Standards and Technology). 2020. "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software." *News*, December 19, 2019, updated May 18, 2020, NIST, US Department of Commerce, Gaithersburg, MD. https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: NYU Press. https://nyupress.org/9781479837243/algorithms-of-oppression.

Noveck, Beth Simone. 2017. "Rights-Based and Tech-Driven: Open Data, Freedom of Information, and the Future of Government Transparency." *Yale Human Rights and Development Law Journal* 19 (1): article 1. https://digitalcommons.law.yale.edu/yhrdlj/vol19/iss1/1.

OECD (Organisation for Economic Co-operation and Development). 2013. *The OECD Privacy Framework*. Paris: OECD. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

OECD (Organisation for Economic Co-operation and Development). 2019a. *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies*. Paris: OECD. https://doi.org/10.1787/276aaca8-en.

OECD (Organisation for Economic Co-operation and Development). 2019b. "Licensing of IP Rights and Competition Law." Background Note DAF/COMP(2019)3, Competition Committee, Directorate for Financial and Enterprise Affairs, OECD, Paris. https://one.oecd.org/document/DAF/COMP(2019)3/en/pdf.

OECD (Organisation for Economic Co-operation and Development). 2019c. "Recommendation of the Council on Artificial Intelligence." *OECD Legal Instruments*, OECD/LEGAL/0449, adopted on May 22, 2019. https://

legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
OneTrust DataGuidance and FPF (Future of Privacy Forum). 2019. "Comparing Privacy Laws: GDPR v. CCPA." OneTrust, London; FPF, Washington, DC. https://fpf.org/wp-content/uploads/2019/12/ComparingPrivacyLaws_GDPR_CCPA.pdf.
Open Knowledge Foundation. 2020. "What Is Open Data?" *Open Data Handbook: Guide.* London: Open Knowledge Foundation. https://opendatahandbook.org/guide/en/what-is-open-data/.
OVIC (Office of the Victorian Information Commissioner). 2020. "Victorian Protective Data Security Framework, Version 2.0." OVIC, Melbourne. https://ovic.vic.gov.au/wp-content/uploads/2020/02/Victorian-Protective-Data-Security-Framework-V2.0.pdf.
Parliament of India. 2019. "The Personal Data Protection Bill, 2019." Bill No. 373 of 2019, Parliament of India, New Delhi. https://dataprotectionindia.in/act/.
PC (Productivity Commission, Australia). 2017. *Data Availability and Use*. Productivity Commission Inquiry Report 82. Canberra: PC. https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf.
PCPD (Office of the Privacy Commissioner for Personal Data, Hong Kong SAR, China). 2012. "Privacy by Design Conference." PCPD, Hong Kong SAR, China. https://www.pcpd.org.hk/pbdconference/index.html.
PMC (Department of the Prime Minister and Cabinet, Australia). 2019. "Best Practice Guide to Applying Data Sharing Principles." PMC, Canberra. https://www.pmc.gov.au/resource-centre/public-data/data-sharing-principles.
Potey, Manish M., C. A. Dhote, and Deepak H. Sharma. 2016. "Homomorphic Encryption for Security of Cloud Data." *Procedia Computer Science* 79 (January): 175–81. https://doi.org/10.1016/j.procs.2016.03.023.
Ragavan, Srividhya, Brendan Murphy, and Raj Davé. 2016. "FRAND v. Compulsory Licensing: The Lesser of the Two Evils." *Duke Law and Technology Review* 14 (1): 83–120.
RIA (Information System Authority, Estonia). 2020. "Data Exchange Layer X-Tee." RIA, Tallinn, Estonia. https://www.ria.ee/en/state-information-system/x-tee.html#:~:text=X%2Dtee%2C%20the%20data%20exchange,data%20based%20on%20an%20agreement.
Smith, Jack, IV. 2016. "Crime-Prediction Tool May Be Reinforcing Discriminatory Policing—Business Insider." *Business Insider*, October 10, 2016. https://www.businessinsider.com/predictive-policing-discriminatory-police-crime-2016-10?r=UK.
Stats NZ (Statistics New Zealand). 2019. "Algorithm Charter." Stats NZ, Wellington, New Zealand. https://data.govt.nz/assets/Uploads/Draft-Algorithm-Charter-for-consultation.pdf.
Sweeney, Latanya. 2000. "Simple Demographics Often Identify People Uniquely." Data Privacy Working Paper 3, Carnegie Mellon University, Pittsburgh.
Sweeney, Latanya. 2002. "k-Anonymity: A Model for Protecting Privacy." *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10 (05): 557–70. https://doi.org/10.1142/S0218488502001648.
Taylor, Linnet, Luciano Floridi, and Bart van der Sloot, eds. 2017. *Group Privacy: New Challenges of Data Technologies.* Philosophical Studies Series, vol. 126. Cham, Switzerland: Springer.
TBS (Treasury Board of Canada Secretariat). 2020. "Responsible Use of Artificial Intelligence (AI)." *Canada.ca*, July 28, 2020, TBS, Ottawa. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html.
TOOP (The Once-Only Principle Project). 2021. "The Once-Only Principle Project." Tallinn University of Technology, Tallinn, Estonia. https://www.toop.eu/about.
Treasury, Australia. 2020. *Inquiry into Future Directions for the Consumer Data Right*. Canberra: Treasury. https://treasury.gov.au/sites/default/files/2020-12/cdrinquiry-accessible final.pdf.
Ubaldi, Barbara. 2013. "Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives." OECD Working Paper on Public Governance 22, Organisation for Economic Co-operation and Development, Paris. https://doi.org/10.1787/5k46bj4f03s7-en.
UNCITRAL (United Nations Commission on International Trade Law). 1998. "UNCITRAL Model Law on Electronic Commerce (1996) with Additional Article 5 bis as Adopted in 1998." UNCITRAL, Vienna. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce.
UNCITRAL (United Nations Commission on International Trade Law). 2001. "UNCITRAL Model Law on Electronic Signatures (2001)." UNCITRAL, Vienna. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures.
UNCITRAL (United Nations Commission on International Trade Law). 2009. *Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods*. Vienna: United Nations. https://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf.
UNSDG (United Nations Sustainable Development Group). 2017. "Data Privacy, Ethics, and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda." UNSDG, New York. https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf.
Vickery, Graham. 2012. "Review of Recent Studies on PSI Re-use and Related Market Developments." Information Economics, Paris.
Ville de Nantes (City of Nantes, France). 2019. "Charte métropolitaine de la donnée" [Metropolitan data charter]. *Nantes Métropole,* May 2019, Ville de Nantes, France. https://metropole.nantes.fr/charte-donnee.
Waze. 2018. "Waze Celebrates 600 Connected Citizens Program Partners." *Waze*, Google, Mountain View, CA. https://medium.com/waze/waze-celebrates-600-connected-citizens-program-partners-36945fbceb66.
WEF (World Economic Forum). 2011. "Personal Data: The Emergence of a New Asset Class." In collaboration with Bain & Company, Inc., WEF, Geneva. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.
Wilkinson, Mark D., Michel Dumontier, IJsbrand Jan Aalbersberg, Gabrielle Appleton, Myles Axton, Arie Baak,

Niklas Blomberg, et al. 2016. "The FAIR Guiding Principles for Scientific Data Management and Stewardship." *Scientific Data* 3 (March 15): 160018. https://doi.org/10.1038/sdata.2016.18.

World Bank. 2018. "Global Indicators of Regulatory Governance: Worldwide Practices of Regulatory Impact Assessments." World Bank, Washington, DC. http://documents1.worldbank.org/curated/en/905611520284525814/Global-Indicators-of-Regulatory-Governance-Worldwide-Practices-of-Regulatory-Impact-Assessments.pdf.

World Bank. 2019. *ID4D Practitioner's Guide: Version 1.0*. October 2019. Washington, DC: World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

World Bank and United Nations. 2017. *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*. Washington, DC: World Bank. http://documents.worldbank.org/curated/en/355401535144740611/Combatting-Cybercrime-Tools-and-Capacity-Building-for-Emerging-Economies.

World Wide Web Foundation. 2017. *Open Data Barometer: Global Report*, 4th ed. Washington, DC: World Wide Web Foundation. https://opendatabarometer.org/doc/4thEdition/ODB-4thEdition-GlobalReport.pdf.

Zanfir-Fortuna, Gabriela, and Sasha Hondagneu-Messner. 2019. "CPDP 2019 Panel: Understanding the Limits and Benefits of Data Portability." Future of Privacy Forum, 2019 Computers, Privacy, and Data Protection Conference, Brussels, February 26, 2019. https://fpf.org/2019/02/26/cpdp-2019-panel-understanding-the-limits-and-benefits-of-data-portability/.

Zhang, Gil, and Kate Yin. 2020. "A Look at China's Draft of Personal Data Protection Law." *Privacy Tracker*, International Association of Privacy Professionals, Portsmouth, NH. https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/.