*Data & Policy* (2022), 4: e25
doi:10.1017/dap.2022.17

RESEARCH ARTICLE

# Building better global data governance

Jacqueline Kuzio[1,*], Mohammad Ahmadi[2], Kyoung-Cheol Kim[3], Michael R. Migaud[2], Yi-Fan Wang[4] and Justin Bullock[5]

[1]Department of Landscape Architecture and Urban Planning, Texas A&M University, College Station, Texas, USA
[2]Institute for Science, Technology and Public Policy, Texas A&M University, College Station, Texas, USA
[3]Department of Public Administration and Policy Athens, University of Georgia, Athens, Georgia, USA
[4]School of Public Administration, University of Nebraska-Omaha, Omaha, Nebraska, USA*
[5]The Bush School of Government & Public Service, Texas A&M University, College Station, Texas, USA
*Corresponding author. E-mail: j-kuzio@tti.tamu.edu

**Received:** 01 April 2021; **Revised:** 01 July 2022; **Accepted:** 08 July 2022

**Key words:** data governance; data protection; data regulation; global governance

## Abstract

In this article, we explore the challenges of global governance and the particular challenge presented by global data governance. We discuss a range of challenges to developing meaningful global governance institutions for regulating how companies and governments around the world manage and utilize consumer data. These challenges are compounded by their global nature and the complexities of Internet-based technologies. We argue that the following gaps exist for effective global data governance: (a) there is no overarching global framework for protecting consumer data, and it is partial and incomplete; (b) there is a lack of data protection for international data transfers, as much of the regulation that is being developed is not global in scale; and (c) new areas of data collection and use compound concerns to effective data governance in a globalized digital world. Moreover, we highlight important needs in terms of both global governance and impending challenges related to current and new uses of data. Any global governance framework should recognize the need for an iterative process where communication is ongoing between the necessary stakeholders. Agreements should incorporate common goals to maximize the potential development of global data governance norms. However, goals must remain flexible to the different data environments across nation-states while maintaining a global scope to ensure data protection. In addition, any agreement should consider the emerging challenges in this area. These challenges include new methods of data collection and use, as well as protecting individuals from manipulation and undue influence based on how their data are being used, processed, and collected.

## Policy Significance Statement

Data governance is gaining importance as more and more data are collected, shared, and disseminated by both the public and private sectors. In a connected, globalized economy, there is a need for data governance to be global. The lack of effective global data governance creates a patchwork of regulation that is difficult for consumers to understand and raises issues of compliance for multinational corporations. This paper provides an overview of the reasons why global data governance is needed and the most pressing issues any framework must consider. Policymakers are already grappling with data privacy and governance issues at the national level, but we argue that a global approach is necessary to ensure adequate protection for individuals.

*The online version of this article has been updated since original publication. A notice detailing the change has also been published.

© The Author(s), 2022. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

## 1. Introduction

The world continues to lag in response to the challenges created by the global digitization of human behavior, both within the digital universe and the analog universe in which we reside. This lag is understandable. The fast pace of technological innovation presents a challenging scenario for governments and governing systems throughout the world. Digitization, and the use of digitized data for machine learning, are unfurling throughout the world at a dramatic pace. This globalized effort has given rise to both surveillance capitalism and dramatic increases in government surveillance throughout the world. This situation suggests that global solutions with international enforcement mechanisms are needed to counter widespread surveillance of individual humans and violation of basic human rights by companies and governments. Relying on private professional self-regulation is not enough to ensure the basic respect for human rights, neither are the efforts of any individual nation or subset of nations.

While the United Nations and other international bodies have begun wrestling with the current global data governance regime, there have been numerous regional- and national-level efforts to regulate the collection and use of digitized data. The most prominent of these efforts has been the European Union's (EU) enactment of the General Data Protection Regulation (GDPR). This regulation has its own weaknesses, as we will discuss, but represents a major step forward in global data governance. For several reasons, the United States has no comprehensive regulatory legislation for data governance. However, the State of California passed the California Consumer Protection Act (CCPA) in 2018. The CCPA was enacted in the wake of the enthusiasm for the GDPR and shares some important similarities with the regulation while also tailoring to its own environment as state legislation. For further global context, we briefly explore other national approaches to data governance from China, Japan, Taiwan, and India.

Through an exploration of the EU and U.S. efforts and an overview of other single-state actors, the opportunities, limitations, and challenges of these regional and national approaches will be discussed. As we will see, in a global digitized world, there exist both externalities in the forms of data collection, analysis, and generation by multinational companies, and each country's own fear of failing to maintain a competitive edge in the global marketplace of digitized data. These challenges make global data governance difficult. Despite this, we do find that governments and international governmental organizations are beginning to carefully discuss and consider regulatory and enforcement possibilities for creating a more effective approach to global data governance. Governance is discussed in this paper as how institutions influence and direct activity in society. Governance frameworks can be well applied to analyze dimensions of policy and administration as well as stakeholder relationships key to governmental functioning at different levels of institutional environments. The framework is applied to deal with multinational dimensions (global governance) and a more specialized focus (e.g., data governance).

If constructed well, global data regulatory regimes could work to reshape the global market and governance strategies that currently allow for the systematic abuse of human rights through the storage and manipulation of digitized data that further manipulate behavior in the analog world. Successful regulation, norms, and standards could rebalance the relationship between individual human rights and the collective interests of private corporations and governments. This paper examines different data governance approaches to address the problems of data harvesting and manipulation on the global stage. A critical review of current global governance approaches provides strong principles, as well as lessons learned that can be applied to the global governance of data. Differing approaches also show the challenges inherent in establishing any governance framework. The key challenges we identify are (a) no overarching framework for the protection of consumer data throughout the life cycle of the data, including data that are processed by information resellers, as well as an overreliance on the principle of "informed consent"; (b) a lack of protection in cases of cross-border and international data transfers that could lead to the lowest standard of protection becoming the norm; and (c) new areas of data collection have a global scope, but no corresponding adequate regulation either at the national or international level. However, these challenges must be overcome if individuals are to retain influence on how their personal information is used to others' ends. The power of ever more digitized data and the ability to analyze it at

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

both superhuman speeds and with superhuman analytical insights gives those who own and control the data the power of the twenty-first century. If good governance and accountability are to hold as core values in the data era, better solutions must be found for our current global data governance system. This will take an effective system that adapts to fast-paced changes in technological capabilities and provides for effective enforcement mechanisms to be determined by impartial expert regulators.

## 2. Global Governance: An Overview

Global governance arose as international problems expanded beyond war and conflict to include a range of "global public goods," such as environmental protection, space exploration, and healthcare (Jang et al., 2016; Zürn, 2018a). In the early days of globalization, the term governance conveyed the lack of hierarchy and indistinct power structures between nation-states (Finkelstein, 1995; Jang et al., 2016; Krisch, 2017). As the international arena has welcomed new and emerging actors, from nation-states taking a greater global role to multinational corporations increasing their wealth, scale, and influence, issues of power, legitimacy, and authority in global governance continue to grow (Zürn, 2018b). Today, global governance has broadened to consider concerns over scientific discoveries and global cyberspace, which often require transnational networks of both state and non-state actors. However, notwithstanding the United Nations, most cooperative agreements across national boundaries rarely rise to the level of global cooperation. Merging competing interests and establishing norms among actors that can range from private companies, governmental organizations, to nation-states themselves requires an establishment of normative principles, a specific institution to house these principles and act as the "authority," as well as structures to guide interactions (Zürn, 2018a). These structures rest on principles of liberalism, cooperation, and coordination between states, and an agreement on mutual goals and interests, but a rise in non-state actors and increased fragmentation and segmentation of the overall governance system can threaten the stability of global governance (Weiss, 2000; Jang et al., 2016; Biermann et al., 2017; Zürn, 2018a). Therefore, if a global governance framework is to be applied to emerging issues, such as data governance, understanding the theoretical underpinnings and the current challenges for these global governance frameworks is key.

### *2.1. Theoretical overview*

Global governance reflects the need to establish authority across national borders to handle common goods or transnational problems. Due to the nature of this relationship, the first step is always communication between nation-states that agree on such common goods or transnational problems (Zürn, 2018b). This agreement is reliant on the establishment of normative principles, which includes consensus on the common good, available authorities that are accountable at the nation-state level, and a belief that international or global authority is plausible (Jang et al., 2016; Zürn, 2018a). Theoretical issues in global governance revolve around authority, legitimacy, and conflict (Weiss, 2000; Zürn, 2018b). Authority relies on institutions for enforcement and legitimacy of these actions; international bodies generally do not have directly elected representatives, which threatens the legitimacy of any enforcement action undertaken. In addition, authority is not strict within a global framework. Due to issues of legitimacy, it is best viewed as being fluid. Fluidity refers to the interplay between state and non-state actors and the nature of cooperative agreements. However, fluid authority is not a common framework for national governance and so it leads to conflict (Krisch, 2017). Conflict naturally arises between actors that make unilateral decisions in their own context and then must compromise on the international stage. Global governance is not restricted to representatives of nation-states either. Non-state actors, such as corporations and agencies directly involved with a common good, can be included within these frameworks. For example, credit rating agencies are a core actor in terms of financial governance and regulation (Jang et al., 2016; Wang, 2017; Zürn, 2018b). While non-state actors can provide expertise and solutions beyond the capacity of individual states, this further raises issues of legitimacy, especially in terms of co-option by special interests. This is one of the enduring challenges of self-regulation by industry.

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

While common problems in global governance involve conflict, coordination, and cooperation, power structures and inequities in power can ultimately be destructive to international bodies or global agreements. The early days of global governance saw international bodies consisting of mostly Western powers. As emerging powers, such as Brazil, Russia, India, and China, entered the space, areas and avenues for conflict increased without any mechanism for increased cooperation (Barnett and Duvall, 2004; Jang et al., 2016; Stephen, 2017). As these emerging powers enter international agreements, segmentation and fragmentation occur. The introduction of new actors may create instability in the global order, but this can also be an opportunity to innovate and determine new norms (Jang et al., 2016; Wang, 2017). Finally, ineffective incorporation of emerging actors creates power imbalances and ultimately abuse by more powerful states. Mechanisms for correcting these power distortions and determining mutually acceptable norms are necessary for successful global governance.

Attempts to address the multiple complex issues that arise in global governance have led to several frameworks being developed. To the extent that this paper aims to provide a brief review of frameworks in global governance. A "framework," for our purposes, takes a set of variables and their presumable relationships together in a conceptual way. Then, this conceptual framework can be further specified toward a "theory" (Ostrom, 2007; Sabatier and Weible, 2007). A theory provides more dense and coherent relationships among variables; yet, the relationships themselves are still susceptible to values of variables, which are yet fully specified. Then, a "model" is much narrower in scope and more precise in its assumptions. In particular, "the framework can provide anything from a modest set of variables to something as extensive as a paradigm" (Sabatier and Weible, 2007), and this can be inevitable, realistically required, and crucial in dealing with, especially, challenging complex issues. Hence, we can first aim to better understand existing frameworks and develop them further by examining current cases for the progress and challenges they illustrate in global data governance. This brief overview can be a significant step moving forward to develop further specified theories and models facing the phenomena.

### *2.2. Frameworks in global governance*

Global governance theory utilizes frameworks that leverage indistinct institutional hierarchies and normative principles to the advantage of the task at hand, whether that be sustainable development, regulating gene editing, or cyberwarfare. This paper will focus on three frameworks that offer potential in terms of global data governance. The frameworks are (a) *governance through goals*, (b) *governance from the ground up*, and (c) *governance by fragmentation.*

*Governance through goals* is presented as a novel approach that was used by the United Nations in developing and implementing their Sustainable Development Goals. The framework differs from traditional global governance approaches by its detachment from the international legal system, its flexibility in terms of adaptation to local needs, and general "weak" power structures (Biermann et al., 2017). The goal-making process aimed to be inclusive of the needs of each nation to better ensure compliance since these goals are non-binding (Murphy and Yates, 2009; Biermann et al., 2017). The success of such an arrangement relies on compliance and formalizing of these goals by each member state, but the flexibility provided increases the probability of integration of global goals into a national context. The ability to adapt to local needs and be flexible in terms of enforcement mechanisms may ultimately lead to slow progress, but it also achieves buy-in from a larger number of members (Thakur and Van Langenhove, 2006). A "governance through goals" approach relies heavily on non-state actors, such as research communities, to determine measurements for progress and whether progress is in fact being made (Biermann et al., 2017). Ultimately, the success of governance through goals relies on inclusivity in process and compliance by individual nation-states.

*Governance from the ground up* focuses on the needs and strategies of local actors and communities and generates an adaptable global governance framework based on those local needs. A bottom-up approach is common across multiple fields, including policy implementation, where the theoretical emphasis lies with target groups or local-level actors rather than actors at the national-level or policy

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

designers (Hjern and Porter, 1981; Matland, 1995; Koontz and Newig, 2014; Meter and Horn, 2016). In terms of global governance, a bottom-up approach has been recommended in the case of gene-editing because local-level actors often have the requisite expertise and can provide a more diverse perspective. There is also the belief that local actors will be free of the conflicts of national policy that can hamper top-down efforts in collaborative decision-making (Kofler et al., 2018). This type of approach does assume weak institutional arrangements since national-level frameworks are being avoided in favor of local knowledge and adaptability. The intent of this framework for global governance is to gain buy-in from the actors that will have to implement any policies or regulations decided upon, so the lack of enforcement mechanisms is viewed as less problematic.

Finally, *governance by fragmentation* acknowledges that governance and governing activities can begin from a patchwork of international institutions and regulations rather than a formalized order (Biermann et al., 2009). The fragmentation framework is based on the idea of global governance as an architecture, which refers to the overall system of public and private institutions, norms, regulations, decision-making apparatus, and organizations that are working on a particular global governance issue (Biermann et al., 2009). Fragmented global governance is not devoid of an architecture in which to govern, but instead, the focus has been less on institutions and centralized control and more on fluid and organically established norms formed not just by state and intergovernmental organizations, but by civil society and non-state actors. The strengths of fragmentation can be seen in the arenas of cyberweapons and cyberwarfare, where the environment is complex, involves many non-state actors with greater technical expertise, and enters into power politics and international relations (Stevens, 2017). One area of fragmentation is existing norms in certain nation-states and the desire in global governance to converge institutions and norms rather than reducing conflict between differing strategies. This can be viewed as a strength and an opportunity for innovative solutions in a space, such as data governance, where strategies currently exist but may not converge.

All these frameworks attempt to wrestle with the international context of weak institutions and weak enforcement mechanisms. This lack of institutional strength may limit the ability to establish norms as well as accountability structures. New global data governance frameworks should address this weakness by establishing norms of enforcement that are mutually agreeable across the globe. Existing regional, national, and inter-country agreements should be harnessed in developing such mechanisms.

### *2.3. Data governance*

With the rapid development of technology, data governance becomes one of the most salient issues for good governance. Data governance emphasizes assigning authorities and building stewards to control and regulate data-related activities, such as data collection, processing, protection, and uses (Janssen et al., 2020). There are many potential actors in data governance, including governments, markets, and civil society. These participants have various interests and preferences to construct different data cultures and infrastructures (Meijer, 2018). Regulations, cultures, policies, principles, and procedures mutually interact with social contexts, expectations, and norms to present diversified natures of data governance in different communities (Meijer, 2018; Janssen et al., 2020). Moreover, public values, such as transparency, accountability, and fairness, are often inherent goals for decision-making in the field of data governance (Chen, 2017). To pursue these goals, data governance mechanisms need to include potential actors, data processes, and public values in the consideration.

Clarifying the dimensions of data governance, Khatri and Brown point out five key data decision domains, such as data principles, data quality, metadata, data access, and data life cycle, which are useful references for global data governance. We highlight two domains on which global data governance should focus. These are data principles that determine how data can be used, reused, shared, and transferred, and data life cycle which refers to data inventory, retention, and retirement (Khatri and Brown, 2010).

First, data principles require governments to establish a concise and effective mechanism to regulate data use, sharing, and exchange (Khatri and Brown, 2010). The rules shape actors' behaviors and further

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

construct the interaction among participants in data governance. Specifically, data principles motivate actors to have various considerations in controlling and planning, risk assessing, data auditing, and monitoring (Janssen et al., 2020).

Second, the data life cycle provides another approach to analyze data governance. One of the issues in data governance is how organizations, including governments, private companies, and third parties, collect personal data. In recent years, as artificial intelligence (AI) and other advanced technologies have become more widely adopted, it is easy to collect personal data but becomes harder to protect the information compared to traditional approaches (Hansen and Porter, 2017).

Furthermore, one of the goals of data governance is to build a trustworthy mechanism to use and protect personal data (Khatri and Brown, 2010; Janssen et al., 2020; Verhulst, 2021). As citizens and customers understand the purposes of data use, the mechanism of data processing, and the life cycle of their personal information, they can have higher levels of trust in sharing data with governments or private entities (Stalla-Bourdillon et al., 2020; 2021). In other words, transparency in data use and processing is pivotal to enhancing trust in data sharing. Furthermore, accountability and responsibility are two essential components of trustworthy data protection regulations (Khatri and Brown, 2010; Verhulst, 2021).

Although the existing body of knowledge provides data principles, data life cycle, and trustworthy mechanisms within domestic data governance, the larger world lacks the authority to build data principles and regulate data life cycle in fact. Countries have their individual data protection regulations, and thus different general data principles are developed. In other words, data regulation and protection depend on the legal regime within individual countries rather than across them.

## 3. Current Regional and National Data Governance Strategies

Despite struggles related to the pace of technological change and a large amount of data in the digital space, countries and regional entities have recently made progress in creating regulations that attempt to increase data privacy and protection as well as connect these with strong enforcement mechanisms to ensure compliance. The EU's adoption of the GDPR has sparked attempts at meaningful data privacy legislation in countries and regions across the globe. Several approaches to data governance will be discussed in this section with a focus on the EU and U.S. legislation.

### *3.1. The European approach*

The GDPR addresses the issue of data privacy for the online activity of EU citizens. It was developed and implemented on April 14, 2016, after decades of discourse on improving existing standards (mainly the "95 Directive") and practices for protecting the personal data of Europeans. Lawmakers incorporated strict enforcement mechanisms to incentivize compliance. The GDPR mandates that entities processing data must comply with seven principles: (a) lawfulness, fairness, and transparency; (b) purpose limitation; (c) data minimization; (d) accuracy; (e) storage limitation; (f) integrity and confidentiality; and (g) accountability (European Parliament and Council of European Union, 2016). Each of these principles provides guidance as to the scope, scale, and type of data that can be processed in certain instances. These requirements also place standards on data processors detailing the level of security that must come with harvesting data. The GDPR requires "appropriate technical and organizational measures" to ensure that data are secure, and that can range from the implementation of dual-factor authentication to end-to-end data encryption techniques (European Parliament and Council of European Union, 2016). The primary objective of this legislation is to govern the ways in which personal data are collected, managed, and erased (European Parliament and Council of European Union, 2016). The EU sought to achieve this goal by developing the GDPR in a way that harmonizes data protection laws across European nations, regulates the transfer of Europeans' personal data outside of Europe, and ultimately gives Europeans greater authority over how their personal data are managed (Houser and Voss, 2018). The GDPR is more powerful than its predecessor (95 Directive) because of its stronger enforcement mechanisms (Houser and Voss, 2018).

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

There are several new protections in the GDPR that were absent from the 95 Directive. One of the most famous protections in the GDPR is the "right to be forgotten." The right to be forgotten or the "right of erasure" allows Internet users to request entities that have collected their data, to delete their data. This issue of whether or not personal data should be harvested by companies gained salience after a 2014 European Court of Justice ruling from a lawsuit between the Internet conglomerate, Google, and the nation of Spain in which the court declared that "European citizens have a right to request that commercial search firms, such as Google, that gather personal information for profit should remove links to private information when asked, provided the information is no longer relevant" (Ilešič, 2014). Another critical protection added to the GDPR is that data processors are legally liable for managing user personal data, while the 95 Directive only held controllers liable. This means if someone were to request their personal data be removed by a controller, then the controller would have to ensure any possible third-party data processors must erase the user's data as well. Other protections include the ability to transfer data between controllers at no cost to the user, the best practice of European companies appointing a Data Protection Officer to manage client data, and the right of users to inquire about how their data are being utilized by data controllers and processors when an "automated decision" is made regarding their data (Houser and Voss, 2018).

One notable departure from the 95 Directive to the GDPR was an increase in the strength of enforcement mechanisms attached to the regulation. The enforcement of the GDPR still relies on individual member states, through their Data Protection Authority (DPA), to coordinate with the European Commission, the newly established European Data Protection Board (EDPB), and other member states. However, now DPAs have much broader powers to investigate and levy heavier fines against companies found to be in violation of the GDPR. DPAs monitor the ability of citizens to exercise their rights under the regulation and evaluate whether the control and processing of personal data by companies are in compliance with the regulation (Tolsma, 2020). Using guidance from the EDPB, DPAs handle cases of suspected violations, assess these claims, and ultimately determine the appropriate penalty. Despite additional guidance being provided, the administering of fines is still largely fragmented by country and each DPA's approach to determining the severity of the violation. Member state laws also play a role in the fragmentation of fines as each country has the ability to set stricter rules than the GDPR (European Commission, 2020).

Although the GDPR intended to increase the strength of enforcement and drive changes in the practices and procedures related to the use of EU citizen data, the lessons learned since 2018 highlight continuing challenges with regulation and compliance, in particular, the GDPR's consistency mechanism, which requires that the supervisory authority in the Member State that a company has indicated as its main establishment must take the lead. Major companies, such as Facebook, Twitter, Apple, and Google, have stated their main establishment to be in Ireland, which has created a significant backlog of cases for Ireland's Data Protection Commission. Other DPAs have complained about this backlog as well as the consistency mechanism, claiming it leads to delays and communication breakdowns (Heine, 2021). Outside of issues with utilizing the enforcement procedures under the GDPR, research has shown that when fines are levied, they tend to be often small, many within the thresholds of laws set prior to the GDPR (Wolff and Atallah, 2021). In addition, only half of the articles that allow for penalties under the GDPR have been utilized with the majority of these relating to privacy protections (Wolff and Atallah, 2021; Ruohonen and Hjerppe, 2022). While privacy protections have led to the greatest number of fines, the largest fines have been levied against security violations (Wolff and Atallah, 2021). Evidence from the first few years of GDPR enforcement shows signs of gradual improvements in terms of company security practices as well as protecting privacy for individuals (Heine, 2021). However, any global framework should take into account the problems of regional consistency and the need for resources to effectively regulate such a law.

### *3.2. The U.S. approach*

The current data privacy protections in the United States are based on a patchwork of laws and regulations across multiple levels of government. Federal law offers protection for certain data and protected classes,

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

and then states often have their own data protection and/or privacy legislation. For example, the Health Insurance Portability and Accountability Act provides protection for medical information, and the Children's Online Privacy Protection Act protects the data of those under the age of 13 (FTC, 2013; Houser and Voss, 2018; O'Connor, 2018; OCR, 2020). In addition, the Family Educational Rights and Privacy Act protects certain student records. Ultimately, the Federal Trade Commission (FTC) is responsible for the enforcement of laws and regulations regarding data privacy and security. The FTC has the power to prohibit "unfair and deceptive trade practices" under Section 5 of the FTC Act (O'Connor, 2018). Attempts have been made in recent years to address the expansion of the digital world and provide consumers with more information about the data being collected as well as protections for their privacy. At the federal level, these efforts have largely involved research through commissions and studies. However, the White House did develop the Consumer Privacy Bill of Rights in 2010 that would have expanded the FTC and state attorney general's authority as well as consumer rights. Initial state efforts started with data breach notification laws and have recently expanded, following the introduction of the GDPR, to address the multitude of concerns related to data collection and control (NCSL, 2020).

### *3.3. The California Consumer Privacy Act and other state efforts*

While the U.S. Congress has yet to pass legislation concerning data privacy and protection, California became the first state to adopt a law comparable to the GDPR in 2018. The CCPA provides several protections for the personal information of Californians. The CCPA affords Californians the right to know if their personal information is being collected as well as the right to access that personal data (California Office of the Attorney General, 2020). It also grants Californians the right to delete data collected from their activity and the ability to opt out of the sale of their data (Camhi and Lyon, 2018; California Office of the Attorney General, 2020). The CCPA is comparable to the GDPR as it exerts its authority on businesses and data processors based, and operating, outside of California. This has serious implications for companies operating around the United States because while California is only one of 50 states, its population of 45 million people accounts for a significant portion of the overall U.S. population, and it has the fifth largest economy on earth (Federal Reserve Bank of St. Louis, n.d.). California's position in the global economy means companies and nations far beyond the state's political borders will face pressure to comply with CCPA regulations.

Several other U.S. states have taken efforts to address data privacy since California passed the CCPA in 2018. Maine and Nevada each enacted data privacy bills into law. The privacy law passed in Maine allows consumers to restrict the types of information companies can collect from their online activity, allows consumers to opt out of their personal information being sold to third parties without their consent, requires companies to explain certain data handling practices to consumers, and prohibits discrimination against consumers that exercise their rights (Rippy, 2020). Nevada's data privacy bill is similar to Maine's in that it provides consumers the right to opt out of their data being sold without their consent, and it requires companies to be transparent about data handling policies (Rippy, 2020). As of this writing, California is the only state in the United States that has adopted a "right to be forgotten" policy like that of the EU's GDPR. Other states have introduced bills that have been rejected or are currently going through the legislative process. Some of these proposed pieces of legislation are similar to the laws passed in Maine and Nevada, with many adopting different policies and protections that include limiting the ability of companies to collect consumer data beyond particular instances, rights for consumers to request outdated or incorrect data be deleted or rectified, and much more (Rippy, 2020).

### *3.4. Additional approaches across the globe*

In 2019, India introduced the Personal Data Protection Bill (PDPB) to address consumer data protection issues. This came after the Supreme Court of India ruled in 2017 that India's constitution gave its citizens the right to privacy, leading Indian policymakers to address issues of data protection. The PDPB would give consumers the right to opt out of their data being sold and analyzed by third parties without their consent. The bill also mandates that personal and critical data must be stored within India. Firms must also

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

create platforms that allow consumers to access and erase their data (Burman and Rai, 2020). PDPB enforcement mechanisms are weaker than the GDPR, as fines for the infringement of data protection are limited to roughly US$2.1 million versus the potential billions of dollars in fines the GDPR allows. A unique characteristic of PDPB is that government entities in India are exempt (Burman and Rai, 2020). As of this writing, India's PDPB has been tabled from further movement in the legislature until it has been studied further by a national commission.

Japan's Act on Protection of Personal Information (APPI) legally protects the personal information of citizens, and this has recently expanded to better protect data privacy online. This expansion was partially to comply with the EU and enable data transfer between the Union and Japan. In 2017, Japan's reformed privacy law came into force; the update applied the law to both foreign and domestic countries that processed the data of Japanese citizens (Simmons, 2019). The update aligned the law with the GDPR and led to the establishment of a cooperative agreement between the EU and Japan in terms of data transfer as well as establishing each entity as having adequate levels of personal data protection. The APPI applies specifically to businesses that collect personal information and requires that they specify the purpose of obtaining such information, prevent the unauthorized loss, disclosure, or destruction of personal data, as well as limit the transfer of data to third parties unless the subject consents (Umeda, 2012). Governmental organizations do not have to comply with the law, in a similar manner to India, but other laws regulate governmental use of personal data (Cooman, 2019). Japan also has previously established rights to privacy through legal decisions, and these overlap with the APPI to provide broader rights to privacy that are not limited to the digital world (Umeda, 2017).

The Taiwanese government enacted the Personal Data Protection Act (PDPA) to enhance privacy and individual information security. The government requires the public sector, private companies, and nonprofit organizations to collect and process data following the regulations of the PDPA. Compared to the GDPR, most data protection principles are like the European approach. However, the government has a decentralized management system to monitor all activities related to data protection. Unlike the GDPR, the central government authority and local governments can protect personal data and fine violators. Furthermore, the government allows entities to transfer data to other countries (Ministry of Justice, 2020). In addition, to enforce Transitional Justice, the government can disclose certain personal information without the limitation of the PDPA. Transitional justice refers to the period from 1945 to 1989, when the Taiwanese people lived under a dictatorship. To explore historical truth and recover victims' rights related to these injustices, the current government can collect, transfer, utilize, research, and publish information on these events, including names and individual behaviors. It is the most notable difference in data protection law compared with other democratic countries.

In China, the government has a number of laws and rules related to personal data protection (Feng, 2019). In 2013, the Ministry of Industry and Information Technology announced Regulations for the Protection of Personal Information of Telecommunications and Internet Users and required all companies to follow this rule. This regulation ensured that personal data could not be used without the consent of the user or for uses beyond the scope of the original agreement. In 2016, the National People's Congress Standing Committee, the highest legislative institute in China, enacted the Cybersecurity Law (CSL) to increase the protection level of personal data and strengthen the central government's power to monitor the Internet. This included a provision similar to the right to be forgotten as it allows an individual to request their data to be deleted if the collector of said data violated the law or the established agreement (Creemers et al., 2018). In addition, the CSL emphasizes transparency of data collection and processing by companies and provides individual rights to correct their data as well as the right to object to processing. The Information Security Technology—Personal Information Security Specification updated by the Standardization Administration of China in March 2020 provides further clarification for business operators in terms of the CSL. While not a law or regulation like the CSL, the security specifications provide guidance for businesses and a standard for the government to assess companies against (Seamons, 2020).

On November 1, 2021, the Personal Information Protection Law went into effect. This establishes the ability to collect data without consent in national emergencies, such as public health crises, so long as

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

other laws permit such collection. The draft also provides web users with the ability to withdraw their information from the collectors. The government can warn and fine violators up to roughly US$7.6 million or 5% of annual revenue (Creemers et al., 2020). Many elements are still to be defined (Cooley, 2021). It should be noted that both the Data Privacy Law and the Personal Information Protection refer to businesses and individuals operating within China, not the Chinese government. Data privacy laws and protections that apply to companies and not government raise greater concerns for citizens. The smart city project in China that has largely been promoted by the national, centralized government collects a vast array of data on a daily basis (Yang and Xu, 2018). In addition to the fact, new data privacy protections do not prohibit government access to those data. The potential surveillance implications of such a model cannot be ignored. The current status of data privacy and personal information protection laws versus the centralized control over data by the government in China raises further challenges to developing a global data protection framework (Wu et al., 2011).

The diversity in legislation from different nations aimed at addressing data governance issues suggests that there are many ways of tackling this issue. Nations do not have the same privacy laws, values, or standards, and some of these differences pose challenges to the development of a global data governance agreement.

## 4. Challenges for Data Governance in a Global Context

While the passage of the CCPA, the GDPR, and the APPI present important first steps in online data privacy and protection, the expansion of multinational corporations simply reinforces the need for a global approach that sets agreed-upon standards on data protection and privacy. The current patchwork of legislation and regulation surrounding data privacy and protection has the following gaps:

1. No overarching framework for the protection of consumer data throughout the life cycle of the data, including data that are processed by information resellers, as well as an overreliance on the principle of "informed consent."
2. A lack of protection in cases of cross-border and international data transfers that could lead to the lowest standard of protection becoming the norm.
3. New areas of data collection have a global scope but no corresponding adequate regulation either at the national or international level.

Data privacy and data protection are paramount in an age where personal information is almost fully digitalized. These challenges are also challenges of generally agreed upon and enforced data principles, and these principles are maintained throughout the life cycle of the data. The current global framework does not do enough to protect the data that are created daily. Most legislation at the national level focuses either on specific organizations or businesses, avoids governmental agencies, and only protects specific types of data, such as health, financial, and data related to minors (Mulligan et al., 2019; U.S. Government Accountability Office, 2019). In addition, the majority of protections in the United States rely on the principle of "informed consent," which, while it plays its own useful role, is insufficient given the number of interactions between an individual and an online entity as well as the complexity of consent agreements required today (Kerry, 2018; O'Connor, 2018). Even certain protected classes of data can enter the unregulated arena; for example, health data that are collected through a healthcare provider is closely protected under HIPPA in the United States, but those same data collected by a wearable device are subject to far less scrutiny. These gaps are largely due to the sectoral approach to privacy that the United States, as well as other countries, has taken; the lack of protection for certain types of data and data processes will have extensive and significant impacts as advanced processes that utilize large amounts of data, such as machine learning, play a greater role in business and organizational decision-making and control.

Uneven data protection regulation presents barriers to both domestic and international trade. When one country has more strict regulations than another, it is harder for the country with fewer regulations to transfer data, services, and goods to a country with heavier regulations on data privacy. This situation is

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

called the "non-tariff barrier" (Martin, 2017). The introduction of the GDPR presented this non-tariff barrier to countries that did not meet the data protection standards required by the EU. This has led countries to update their privacy and data protection laws to re-establish or maintain the flow of data between the EU and their countries (Martin, 2017). If a global governance structure does not address the differing data protection standards between nation-states, countries that cannot meet the standards will be cut from the global data exchange or standards will shift to the lowest common denominator, risking the protection of privacy that the regulations intended to preserve.

Data are being collected and used in new and nontraditional ways that expand beyond individual nations. This creates additional challenges for countries that wish to protect the data of their citizens. One of these new areas of data collection is through satellites in outer space. Traditionally, as stated by the United Nations' treaties, outer space is treated as a public space, and in some countries, the sky is considered a public space. In theory and practice, any individual or state can collect the data of the individuals on the surface of the earth from orbit. These data are usually collected by remote sensing technologies such as by satellites orbiting the earth. Currently, hundreds of satellites are watching human activities from the orbit of the earth. A satellite constellation that is being run and managed by Planet, for example, soon will have the capacity to revisit certain locations on earth 12 times per day with high-resolution cameras (Ryswyk, 2020). Legally, the collection of these types of data does not require the consent of sensed individuals or states. This is one example of the main emerging data challenges that are not currently addressed by efforts to protect data and privacy at the national and supranational levels.

Remaining anonymous will likely pose an extreme challenge for data governance as well as for the GDPR. Humans already live in a heavily connected world in which a wide range of smart devices consumes individual data with minimum or no human intervention. For example, in the Internet of Things (IoT), many familiar surrounding objects—like home appliances—are connected in one form or another by the Internet (Gubbi et al., 2013). Several interconnected devices make it likely impossible to remain anonymous. Indeed, the full development of IoT "may put a strain on the current possibilities of anonymous use of services" and might lead to unseen "privacy issues and vulnerabilities" (Solangi et al., 2018).

Finally, data themselves are also being used in new and powerful ways. One example of this is the role data play in training machine learning and AI systems. While satellite data provide surveillance from the skies, digital data and algorithmic decision-making models have provided for unparalleled surveillance into our personal lives through our smartphones, our purchasing history, and our social media behavior. In this way, new uses of data have led to mass surveillance of individuals, both by their government and the companies with which they interact, sometimes as consumers and sometimes as inputs to the recommendation algorithms. In addition to these mass forms of global surveillance, data are also being used by government and private companies to make countless decisions about the human being these institutions contain and interact with, including decisions about hiring, prosecuting, and serving, sometimes resulting in administrative evil (Zuboff, 2018; Bullock, 2019; Bullock et al., 2020; Young et al., 2021).

## 5. Discussion

Data governance in the digital era is a global challenge, which requires an effective global governance approach. Unfortunately, to date, effective global data governance has been lacking. Comprehensive digital data regulation is lacking throughout the world, and early national and regional attempts, while in progress, still suffer many governance challenges. As noted in the previous section, global data governance is currently lacking in at least three ways: (a) no overarching framework for the protection of consumer data throughout the life cycle of the data, including data that are processed by information resellers, as well as an overreliance on the principle of "informed consent"; (b) a lack of protection in cases of cross-border and international data transfers that could lead to the lowest standard of protection becoming the norm; and (c) new areas of data collection have a global scope but no corresponding adequate regulation either at the national or international level. These challenges represent a subset of the challenges that can limit effective global governance more generally. These challenges include differing

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

normative principles, definitions of the common good, and institutional control, as well as common global governance challenges that revolve around communication, legitimacy, and collaboration. Finally, these issues are only exacerbated by impending challenges such as new methods of data collection, machine learning, and differing expectations of privacy.

### *5.1. Comparison of data governance approaches*

National, subnational, and supranational regional governing bodies have begun efforts to govern digital data more effectively. These attempts include Japan and Taiwan at the national level, California at the subnational level, and the EU at the supranational level. These early attempts have taken different areas of emphasis, levels of governmental accountability, strength of enforcement, and strength of privacy of personal data and protection of human rights. Again, these are only early efforts, and a systematic approach has yet to emerge, but they are important early efforts. These early efforts have sought to establish legal precedent and regulatory infrastructure for building a global strategy. Global governance theories offer insight into how these emerging regional, national, and state regulations influence overall effective global governance.

An important observation from most of the countries' national data protection laws discussed earlier is that the protection efforts are national laws that canvass all subregions of the country. This allows little interpretation about how data should be protected in different parts of Japan, India, and other nations addressing data privacy issues. The United States is in a more complicated situation now that California has enacted its own data protection law because the federal government must pass a data protection law at least as stringent as the CCPA for the law to be "equal" among all other states. Imbalanced data protection laws can be detrimental to domestic and international trade. If data protection laws are adopted and enforced multilaterally, there are potential complications on how to interpret data privacy issues arising from interactions that fall under multiple jurisdictions. A unilateral, data protection policy that is agreed to by all parties under the laws' jurisdiction would minimize confusion and conflict originating from differing laws. A national or global policy on the governance of digital data would also protect those whose governments do not have the political capital or will to pass such legislation.

While there might not be a defined "best practice" for how to protect consumer data, the EU's GDPR has set the standard for large-scale data privacy laws. As nations around the world continue to develop consumer data privacy policies to protect their citizens from cybersecurity threats, robocalls, and unwarranted data harvesting, one should expect to see nation-states continuing to model their data privacy laws after principles detailed in the GDPR. One might also expect nation-states where the freedom of speech and press are absent or substantially weaker than those rights in more democratic countries to be less likely to: (a) provide exemptions to data privacy rules to their government to provide public leaders the ability to target political dissidents; or (b) pass data privacy legislation at all. India is an important example of this point as the nation's proposed data protection law, the PDPB, exempts the government from following certain provisions within the law. If this provision were to be adopted in other, less-democratic nations, the citizens of that nation could be punished based on their Internet traffic.

Different standards of privacy and protection in individual nations speak to the need for a global data governance system. Current protections focus on the rights of the individuals within these nations leaving that outside without adequate data rights. Requiring corporations that operate within a certain jurisdiction to comply even if they are not based within that jurisdiction expands the reach of these laws, but still fails to protect nations that do not have the institutional capacity to enact their own regulation. In addition, governmental organizations may be able to circumvent regulations, while the focus remains on corporations and businesses that handle data. Understanding the points of agreement and departure between existing regulations is required to begin the move toward a global framework. Global data governance must face and address challenges related to the institutional structure and good governance principles by leveraging the mutually agreed-upon principles of data governance shown in these approaches.

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

### *5.2. Compounding global governance challenges*

The presence of multilateral agreements presents an opportunity to merge currently fragmented regulation into a cohesive global data governance framework. Actors, of various types, can leverage existing agreements and determine key principles, norms, and goals that are present in a variety of data protection laws today. Any framework should also recognize the importance of including multiple actors that have the potential to shape and refine existing norms and principles, as well as provide technical understanding beyond the traditional governmental partners in global governance. Non-state actors will likely be the implementers of many global data governance principles and regulations, so involving them in the initial conversation increases the probability of enforcement. These non-state actors include professional organizations, scientists, and civil society more generally. For example, professional organizations and the broader scientific community play important roles in spotlighting the evolving data governance needs and raising general awareness of the issues. Scientists and engineers themselves play large roles in innovating and implementing agreed-upon data principles for the data throughout its life cycle. In addition, lessons should be learned from attempts to "solve" or work on other global problems or regulation of global common goods. Nation-states can determine the potential for bottom-up governance that focuses on local knowledge and needs rather than imposing strict regulations that fail to understand the regional context. Any global framework must rest on good governance principles, coordination, collaboration, and multilateral decision-making. A global data governance framework will be no different. Although data governance principles already exist in various parts of the world, the challenge is bringing together these efforts into a systematic approach to data governance at the global level.

Addressing global data governance requires mutually agreed-upon goals regarding protection and privacy. While the existence of individual and multi-country laws and inter-country agreements provides a starting point for collaboration, it may also hinder cooperation with states that do not already have these laws or regulations in place. Establishing standards for data protection and privacy will rely on cooperation between nation-states with different cultural expectations of data protection, as well as different capacities to manage and enforce regulations. A global body, like the United Nations, would need to be responsible for merging these competing expectations and monitoring issues of enforcement and compliance. While no truly global data governance effort has been made to date, the passage of the GDPR required countries outside the EU to meet certain standards to interact with EU citizen data. This patchwork of international cooperation is setting the GDPR as the standard for data protection. However, it also leaves anyone outside of the GDPR's framework without that level of protection.

### *5.3. Impending challenges*

Patchworks of cooperative agreements present challenges for nations and multinational corporations that must account for differing standards across borders. Although challenges exist, a global governance framework would provide better data privacy and protection against malicious data collection and manipulation techniques as well as establish globally agreed-upon standards that corporations and other actors can follow. Solutions to existing challenges will only become more crucial as Internet technologies continue to innovate and become increasingly integral to the global economy.

Despite a normative consensus over personal data protection, different political systems have a different operational understanding of privacy. In Europe, the processing of personal information is prohibited unless the data subject has consented or expressly allowed by law (European Parliament and Council of European Union, 2016). In China, however, according to the "Personal Information Protection Law" draft, the personal data could be collected without the consent of the data subject in case of public health incident, for fulfilling statutory duties, for the sake of public interests, and for administrative reasons (Creemers et al., 2020). As the world becomes more interconnected by multinational companies, harmonizing these different operational understandings of privacy, as one form of personal data protection, within different political systems will be a future challenge for policymakers globally.

Finally, not only are personalized, digitized, location- and time-stamped data becoming ubiquitous, these data can be manipulated, analyzed, and used to make increasingly accurate observations and

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

predictions about the world around us. The growing bank of personal data is being exploited by intelligent machines and hybrid intelligence to learn more about the world. Personal data are already being used, en masse, by both large multinational corporations and political actors to shape our collective behavior by using our data to surveil us in such detail that the algorithms can predict our behaviors better than we can ourselves (Zuboff, 2018). This suggests that as effective global data governance evolves, and learning occurs, the challenges are already evolving from concerns about collection and storage to the resulting powers of predictions and behavior shaping by algorithms (Christian, 2020).

## 6. Conclusion

*Good governance* is no easy task. Data governance presents many political and technical challenges for good governance, and when the governance challenge has evolved into a globally connected world that is interconnected in large part by the transmission of digital data, good governance becomes even more challenging. To illustrate and explore these challenges, we have examined the global governance literature and theory for guidance. Building from this background, we examined the current major data governance approaches at the supranational, national, and sub-national levels for solutions and remaining challenges for effective data governance. From there, the impending challenges for effective global data governance were examined.

This process has illustrated the sheer complexity of effective global data governance, and for that matter, the complexity of tradeoffs across individual regulatory efforts. However, despite the complexity, basic effective governance and global governance approaches still provide guidance on an accountable and inclusive governing approach that fosters effective collaboration, coordination, and communication. Establishing common goals, building on current agreements, and utilizing technical expertise where possible and necessary are all key to establishing global data governance. These elements must be combined with strong institutions that reflect the needs of each nation. Leading such an effort will require a focus on good governance principles and ensuring that the governance framework meets the expectations of those involved in crafting the framework.

Given what we know about both global governance and data governance we see, much stronger global efforts are needed for a more effective global data governance regime. We identified that global governance approaches contain at least three major guiding frameworks. These include global governance that is through goals, bottom-up, and by-fragmentation. Each of these approaches has strengths and weaknesses, but taken together as guiding strategies, they have not been completely effective in the domain of global data governance. Focusing on data principles and the life cycle of data, in particular, and through the course of examining use cases throughout the world, we identify at least three ongoing challenges for building better global data governance systems. These include:

1. No overarching framework for the protection of consumer data throughout the life cycle of the data, including data that are processed by information resellers, as well as an overreliance on the principle of "informed consent."
2. A lack of protection in cases of cross-border and international data transfers that could lead to the lowest standard of protection becoming the norm.
3. New areas of data collection have a global scope but no corresponding adequate regulation either at the national or international level.

Through concerted global efforts, data governance can more effectively balance the interest of all stakeholders, encourage accountability, and work toward a sustainable data ecosystem that makes brilliant use of the capabilities of the data era while also taking careful consideration of the risks to society and who bears them. It is also important to note that the global governance landscape with respect to data governance is evolving as well. Much of the challenge is already pointing toward what can already be done with digital data to influence humans. These gaps need to be remedied so that these new and growing challenges may be addressed upon a stronger foundation of better global data governance systems.

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

**Funding Statement.** This research does not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

**Competing Interests.** The authors declare no competing interests exist.

**Author Contributions.** Conceptualization: J.B.; Supervision: J.K. and J.B.; Writing—original draft: all authors; Writing—reviewing and editing: J.K. and M.M.

**Data Availability Statement.** Data availability is not applicable to this article as no new data were created or analyzed in this study.

## References

**Barnett M and Duvall R** (2004) *Power in Global Governance*. Cambridge: Cambridge University Press.

**Biermann F**, **Kanie N and Kim RE** (2017) Global governance by goal-setting: The novel approach of the UN sustainable development goals. *Current Opinion in Environmental Sustainability 26–27*, 26–31. https://doi.org/10.1016/j.cosust.2017.01.010

**Biermann F**, **Pattberg P**, **Van Asselt H and Zelli F** (2009) The fragmentation of global governance architectures: A framework for analysis. *Global Environmental Politics 9*(4), 14–40.

**Bullock J**, **Young MM and Wang YF** (2020) Artificial intelligence, bureaucratic form, and discretion in public service. *Information Polity 25*(4), 491–506.

**Bullock JB** (2019) Artificial intelligence, discretion, and bureaucracy. *The American Review of Public Administration 49*(7), 751–761.

**Burman A and Rai S** (2020) *What is in India's Sweeping Personal Data Protection Bill?* Carnegie India. Available at https://carnegieindia.org/2020/03/09/what-is-in-india-s-sweeping-personal-data-protection-bill-pub-80985 (accessed 17 December 2020).

**California Office of the Attorney General** (2020) *California Consumer Privacy Act (CCPA).* Available at https://oag.ca.gov/privacy/ccpa (accessed 17 December 2020).

**Camhi R and Lyon S** (2018) What is the California Consumer Privacy Act? *Risk Management 65*(9). Available at http://www.rmmagazine.com/articles/article/2018/10/01/-What-Is-the-California-Consumer-Privacy-Act- (accessed 28 July 2022).

**Chen Y-C** (2017) *Managing Digital Governance: Issues, Challenges, and Solutions*. New York: Routledge.

**Christian B** (2020) *The Alignment Problem: Machine Learning and Human Values*. New York: W. W. Norton & Company.

**Cooley** (2021) *China's New National Privacy Law: The PIPL.* Cooley. Available at https://www.cooley.com/news/insight/2021/2021-11-30-china-new-national-privacy-law (accessed 26 June 2022).

**Cooman GD** (2019) *Before GDPR: Japan's Act on the Protection of Personal Information (APPI).* Proxyclick. Available at https://www.proxyclick.com/blog/before-gdpr-japans-act-on-the-protection-of-personal-information-appi (accessed 21 September 2020).

**Creemers R**, **Shi M**, **Dudley L and Webster G** (2020) *China's Draft "Personal Information Protection Law" (Full Translation).* New America. Available at http://newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/ (accessed 12 November 2020).

**Creemers R**, **Triolo P and Webster G** (2018) *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017).* New America. Available at http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (accessed 17 December 2020).

**European Commission** (2020) Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition — Two years of application of the General Data Protection Regulation. Communication from the Commission to the European Parliament and Council. Directorate-General for Justice and Consumers

**European Parliament and Council of European Union** (2016) Regulation (EU) 2016/679. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN (accessed 17 December 2020).

**Federal Reserve Bank of St. Louis** (n.d.) *Total Gross Domestic Product for California.* FRED. Available at https://fred.stlouisfed.org/series/CANGSP (accessed 19 November 2020).

**Feng Y** (2019) The future of China's personal data protection law: Challenges and prospects. *Asia Pacific Law Review 27*(1), 62–82.

**Finkelstein LS** (1995) What is global governance? *Global Governance 1*(3), 367–372.

**FTC** (2013) *Children's Online Privacy Protection Rule ("COPPA").* Federal Trade Commission. Available at https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (accessed 26 August 2020).

**Gubbi J**, **Buyya R**, **Marusic S and Palaniswami M** (2013) Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems 29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

**Hansen HK and Porter T** (2017) What do big data do in global governance? *Global Governance 23*(1), 31–42. https://doi.org/10.1163/19426720-02301004

**Heine I** (2021) *3 Years Later: An Analysis of GDPR Enforcement.* Center for Strategic & International Studies. Available at https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement (accessed 27 June 2022).

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

**Hjern B and Porter DO** (1981) Implementation structures: A new unit of administrative analysis. *Organization Studies 2*(3), 211–227. https://doi.org/10.1177/017084068100200301

**Houser K and Voss WG** (2018) GDPR: The end of Google and Facebook or a new paradigm in data privacy? *Richmond Journal of Law & Technology 25*(1), 1–109.

**Ilešič M** (2014) European Court of Justice, C-131/12.

**Jang J**, **McSparren J and Rashchupkina Y** (2016) Global governance: Present and future. *Palgrave Communications 2*(1), 1–5.

**Janssen M**, **Brous P**, **Estevez E**, **Barbosa LS and Janowski T** (2020) Data governance: Organizing data for trustworthy artificial intelligence. *Government Information Quarterly 37*(3), 101493. https://doi.org/10.1016/j.giq.2020.101493

**Kerry CF** (2018) *Filling the Gaps in US Data Privacy Laws.* Brookings. Available at https://www.brookings.edu/blog/techtank/2018/07/12/filling-the-gaps-in-u-s-data-privacy-laws/ (accessed 9 September 2020).

**Khatri V and Brown CV** (2010) Designing data governance. *Communications of the ACM 53*(1), 148–152.

**Kofler N**, **Collins JP**, **Kuzma J**, **Marris E**, **Esvelt K**, **Nelson MP**, **Newhouse A**, **Rothschild LJ**, **Vigliotti VS**, **Semenov M**, **Jacobsen R**, **Dahlman JE**, **Prince S**, **Caccone A**, **Brown T and Schmitz OJ** (2018) Editing nature: Local roots of global governance environmental gene editing demands collective oversight. *Science 362*(6414), 527–529. https://doi.org/10.1126/science.aat4612

**Koontz TM and Newig J** (2014) From planning to implementation: Top-down and bottom-up approaches for collaborative watershed management. *Policy Studies Journal 42*(3), 416–442.

**Krisch N** (2017) Liquid authority in global governance. *International Theory 9*(2), 237–260. https://doi.org/10.1017/S1752971916000269

**Martin BA** (2017) The unregulated underground market for your data: Providing adequate protections for consumer privacy in the modern era. *Iowa Law Review 105*, 865–900.

**Matland RE** (1995) Synthesizing the implementation literature: The ambiguity-conflict model of policy implementation. *Journal of Public Administration Research and Theory 5*(2), 145–174.

**Meijer A** (2018) Datapolis: A public governance perspective on "smart cities". *Perspectives on Public Management and Governance 1*(3), 195–206. https://doi.org/10.1093/ppmgov/gvx017

**Meter DSV and Horn CEV** (2016) The policy implementation process: A conceptual framework. *Administration & Society 6*, 445–488. https://doi.org/10.1177/009539977500600404

**Ministry of Justice** (2020) *The Comparison of the GDPR and the Taiwanese Data Protection Regulations.* Taiwan Ministry of Justice. Available at https://www.ndc.gov.tw/Content_List.aspx?n=92A54D2FBC1D329E (accessed 20 December 2020).

**Mulligan SP**, **Freeman WC and Linebaugh CD** (2019) *Data Protection Law: An Overview*, March, 79.

**Murphy CN and Yates J** (2009) *The International Organization for Standardization (ISO): Global Governance through Voluntary Consensus*. New York: Routledge.

**NCSL** (2020) *Security Breach Notification Laws.* National Conference of State Legislatures. Available at https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (accessed 26 August 2020).

**O'Connor N** (2018) *Reforming the U.S. Approach to Data Protection and Privacy.* Council on Foreign Relations. Available at https://www.cfr.org/report/reforming-us-approach-data-protection (accessed 26 August 2020).

**Office for Civil Rights U.S. Department of Health and Human Services** (2020) *Your Rights Under HIPAA.* HHS.gov. Available at https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html (accessed 26 August 2020).

**Ostrom E** (2007) Challenges and growth: The development of the interdisciplinary field of institutional analysis. *Journal of Institutional Economics 3*(3), 239–264. https://doi.org/10.1017/S1744137407000719

**Rippy S** (2020) *US State Comprehensive Privacy Law Comparison.* International Association of Privacy Professionals. Available at https://iapp.org/resources/article/state-comparison-table/ (accessed 17 December 2020).

**Ruohonen J and Hjerppe K** (2022) The GDPR enforcement fines at glance. *Information Systems 106*, 101876. https://doi.org/10.1016/j.is.2021.101876

**Ryswyk MV** (2020) *Planet Announces 50 cm SkySat Imagery, Tasking Dashboard and Up to 12x Revisit.* Available at https://www.planet.com/pulse/tasking-dashboard-50cm-12x-revisit-announcement/ (accessed 7 November 2020).

**Sabatier PA and Weible CM** (2007) The advocacy coalition framework: Innovations, and clarifications. In *Theories of the Policy Process*. Sabatier PA. Routledge. Boulder, CO: Westview. pp. 189–222.

**Seamons R** (2020) *China's Personal Information Specifications: Revised.* China Law Blog. Available at https://www.chinalawblog.com/2020/07/chinas-personal-information-specifications-revised.html (accessed 17 December 2020).

**Simmons D** (2019) *9 Countries with GDPR-like Data Privacy Laws.* Comforte Insights. Available at https://insights.comforte.com/9-countries-with-gdpr-like-data-privacy-laws (accessed 18 September 2020).

**Solangi ZA**, **Solangi YA**, **Chandio S**, **Aziz MbtSA**, **Hamzah MSbin**, **Shah A** (2018) The future of data privacy and security concerns in Internet of Things. In: *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*. IEEE, New York City, New York. pp. 1–4.

**Stalla-Bourdillon S**, **Carmichael L and Wintour A** (2021) Fostering trustworthy data sharing: Establishing data foundations in practice. *Data & Policy 3*. E4. https://doi.org/10.1017/dap.2020.24

**Stalla-Bourdillon S**, **Thuermer G**, **Walker J**, **Carmichael L and Simperl E** (2020) Data protection by design: Building the foundations of trustworthy data sharing. *Data & Policy 2*, 1–10.

**Stephen MD** (2017) Emerging powers and emerging trends in global governance. *Global Governance: A Review of Multilateralism and International Organizations 23*(3), 483–502.

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press

**Stevens T** (2017) Cyberweapons: An emerging global governance architecture. *Palgrave Communications 3*(1), 1–6. https://doi.org/10.1057/palcomms.2016.102

**Thakur R and Van Langenhove L** (2006) Enhancing global governance through regional integration. *Global Governance: A Review of Multilateralism and International Organizations 12*(3), 233–240.

**Tolsma A** (2020) *GDPR-Data Protection Authority Enforcement Methods.* Deloitte Switzerland. Available at https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-data-protection-authority-enforcement-methods.html (accessed 4 August 2020).

**U.S. Government Accountability Office** (2019) *Consumer Privacy: Changes to Legal Framework Needed to Address Gaps.*

**Umeda S** (2012) Online Privacy Law: Japan | Law Library of Congress. Available at https://www.loc.gov/law/help/online-privacy-law/2012/japan.php (accessed 21 September 2020).

**Umeda S** (2017) Online Privacy Law: Japan | Law Library of Congress. Available at https://www.loc.gov/law/help/online-privacy-law/2017/japan.php (accessed 21 September 2020).

**Verhulst SG** (2021) Reimagining data responsibility: 10 new approaches toward a culture of trust in re-using data to address critical public needs. *Data & Policy 3*, 1–11.

**Wang H** (2017) New multilateral development banks: Opportunities and challenges for global governance. *Global Policy 8*(1), 113–118. https://doi.org/10.1111/1758-5899.12396

**Weiss TG** (2000) Governance, good governance and global governance: Conceptual and actual challenges. *Third World Quarterly 21*(5), 795–814.

**Wolff J and Atallah N** (2021) Early GDPR penalties: Analysis of implementation and fines through May 2020. *Journal of Information Policy 11*, 63–103. https://doi.org/10.5325/jinfopoli.11.2021.0063

**Wu Y**, **Lau T**, **Atkin DJ and Lin CA** (2011) A comparative study of online privacy regulations in the U.S. and China. *Telecommunications Policy 35*(7), 603–616. https://doi.org/10.1016/j.telpol.2011.05.002

**Yang F and Xu J** (2018) Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law. *Asia & the Pacific Policy Studies 5*(3), 533–543. https://doi.org/10.1002/app5.246

**Young MM**, **Himmelreich J**, **Bullock JB and Kim KC** (2021) Artificial intelligence and administrative evil. *Perspectives on Public Management and Governance 4*(3), 244–258.

**Zuboff S** (2018) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 1st Edn. New York: Public Affairs.

**Zürn M** (2018a) Contested global governance. *Global Policy 9*(1), 138–145. https://doi.org/10.1111/1758-5899.12521

**Zürn M** (2018b) *A Theory of Global Governance: Authority, Legitimacy, and Contestation*. Oxford: Oxford University Press.

**Cite this article: Kuzio J, Ahmadi M, Kim K.-C, Migaud M. R, Wang Y.-F and Bullock J** (2022). Building better global data governance. *Data & Policy*, 4: e25. doi:10.1017/dap.2022.17

https://doi.org/10.1017/dap.2022.17 Published online by Cambridge University Press