Policy Research Working Paper 9594

World Development Report 2021

Background Paper

Achieving Privacy

Costs of Compliance and Enforcement of Data Protection Regulation

Anupam Chander
Meaza Abraham
Sandeep Chandy
Yuan Fang
Dayoung Park
Isabel Yu

WORLD BANK GROUP
World Development Report 2021 Team
&
Macroeconomics, Trade and Investment Global Practice
March 2021

Policy Research Working Paper 9594

Abstract

Is privacy a luxury for the rich world? Remarkably, there is a dearth of literature evaluating whether data privacy is too costly for companies to implement, or too expensive for governments to enforce. This paper is the first to offer a review of surveys of costs of compliance, and to summarize national budgets for enforcement. The study shows that while privacy may indeed prove costly for companies to implement, it is not too costly for governments to enforce. This study will help inform governments as they fashion and implement privacy laws to address the "privacy enforcement gap"—the disparity between the privacy on the books, and the privacy on the ground.

This paper is a product of the World Bank's *World Development Report 2021* Team in collaboration with the Macroeconomics, Trade and Investment Global Practice. It is part of a larger effort by the World Bank to provide open access to its research and make a contribution to development policy discussions around the world. Policy Research Working Papers are also posted on the Web at http://www.worldbank.org/prwp. The authors may be contacted at ac1931@georgetown.edu.

Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation

Anupam Chander,[*] Meaza Abraham,[**] Sandeep Chandy,[***]
Yuan Fang,[****] Dayoung Park,[*****] and Isabel Yu[******]

Keywords: data protection, privacy, globalization, trade, WTO
JEL codes: F13, F15, K20, K24, L86

This paper is a joint product of the WDR 2021 team and the International Trade Unit (ETIRI) of the Macroeconomics, Trade, and Investment GP. The study was commissioned as a background paper to the WDR 2021 "*Data For Better Lives*" and an input to ETIRI's work program on Digital Trade Regulation (P171481), under the guidance of Martín Molinuevo (Senior Counsel, ETIRI).

[*] Professor of Law, Georgetown University. This study was commissioned by the World Bank, in connection with their research towards the World Development Report 2021, which will focus on "Data for Better Lives." We thank the many experts across the world who took the time to speak with us.

[**] University of Northern Colorado, B.A. 2018; Georgetown University Law Center, J.D. expected 2022.

[***] O.P. Jindal Global University, LL.B. 2017; Georgetown University Law Center, LL.M. 2020; Fellow, New Markets Lab, Washington, D.C.

[****] East China University of Political Science and Law, LL.B. 2018; Georgetown University Law Center, J.D. expected 2021.

[*****] University of California, Los Angeles, B.A. 2014; Georgetown University Law Center, J.D. expected 2021.

[******] Wellesley College, B.A. 2017; Georgetown University Law Center, J.D. expected 2022.

Introduction

Is privacy a luxury for the rich world?[1] This paper seeks to understand how much data privacy laws cost to implement and enforce. Relying on industry surveys, government studies, and government agency budgets, this paper compares the costs of private sector implementation and public sector enforcement for the United States, European Union, and, to a limited extent, China. We conclude that data privacy is not outside the reach of the poorer parts of the world, though the rules should be written with differing resources for compliance and enforcement.

The focus of this project is to help provide the informational base needed to support the practical realization of data privacy protections. Like some other legal domains, data privacy laws are subject to an "enforcement gap"—"that is, a wide disparity between the stated protections on the books and the reality of how companies respond to them on the ground."[2] A decade ago, Kenneth Bamberger and Deidre Mulligan observed that "no one has conducted a sustained inquiry into how corporations actually manage privacy and what motivates them."[3] Their study helped understand how companies were responding to regulations and enforcement. But even a decade later, we know too little about the costs of compliance or the costs of enforcement. Despite the rapid embrace of laws designed to regulate the use of personally identifiable information, there is a remarkable scarcity of studies of their costs.[4] The absence of data makes it difficult to assess possible regulatory measures in the area. Some in developing nations may be worried about the costs for small and medium-sized companies of compliance with new regulations. Governments too may also be concerned about the additional costs of enforcement of new laws.

This study begins to fill that lacuna by describing the costs of compliance with data privacy laws for businesses and the costs of enforcement for governments. By focusing on costs, the study should not be read in any way to neglect benefits. A wide array of scholarship and experience has shown that privacy regulations have widespread benefits.[5] Indeed, the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the Charter of Fundamental Rights of the European Union all declare privacy a fundamental human right.[6] Benefits of data privacy are

[1] Julia Angwin, *Has Privacy Become a Luxury Good?*, N.Y. Times, Mar. 4 2014.

[2] Filippo Lancieri, *Narrowing Data Protection's Enforcement Gap* (unpublished manuscript, dated Jan. 2021) (on file with author).

[3] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 249 (2011).

[4] We discuss the existing studies in Part II below. This paper relies on a number of different sources. The principal sources are the laws and regulations of the United States, the European Union, and China, scholarly and professional studies of the operation of the privacy regimes of these three jurisdictions, and government reporting on budgets in these jurisdictions. We supplemented these sources with both expert interviews and a survey that we designed and circulated.

[5] Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 408 (2008) ("The core of intellectual privacy is the freedom of thought and belief."); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1905 (2013) (arguing that, among other things, privacy is "foundational to the practice of informed and reflective citizenship"); Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442 (2016) (reviewing economic literature on privacy).

[6] Universal Declaration of Human Rights, G.A. Res. 217(III)A, art. 8, U.N.Doc A/RES/217(III) (Dec. 10, 1948); International Covenant on Civil and Political Rights, opened for signature Dec. 16, 1966, S. Exec. Doc. E, 95-2 (1978), 999 U.N.T.S. 171 (entered into force Mar. 23, 1976); Charter of Fundamental Rights of the European Union: 2010 O.J. (C83) 389. Proclaimed by the Commission, 7 December 2000.

difficult to quantify outside clear invasions like identity theft.[7] Not only does data privacy have enormous benefits for individuals, it helps companies build and maintain the trust of both their users and their business partners. Indeed, understanding the costs of compliance and enforcement will better enable developing countries to design their laws and enforcement structures.

Understanding the costs of compliance and enforcement is critical to both designing laws and to enforcing them. Across the world, nations are establishing data privacy rules.[8] The datafication of the economy means that few companies or individuals are untouched. Laws regulating the use of personally identifiable data are a necessary foundation of the digital economy. Companies are collecting data at an unprecedented rate, as computers mediate more and more of our lives. Laws help prevent abuse and thus help build trust as individuals interact in an increasingly digitized world. Data privacy is a necessity not just in richer nations, but in poorer ones as well.

Achieving data privacy presents special challenges in the developing world—both for companies and governments. Micro, small and medium-sized companies may lack the resources to ensure compliance with complicated laws. If compliance is too expensive, businesses will simply ignore the law or avoid the jurisdiction altogether. Governments, their resources already stretched, may not be able to devote sufficient resources for privacy enforcement.

Data privacy is also increasingly critical to international trade. As data travels across the world, governments and individuals seek to ensure that privacy protections travel alongside. At the same time, data regulations can be used to disfavor foreign service providers; data regulations that mandate data localization impose special costs.[9]

We focus here on three specific data privacy regimes, the European Union, the United States, and China. Because of their large economies, these data privacy regimes have global influence. The study seeks to elaborate and quantify the costs of data regulations, recognizing the limitations of the data available. Because the European Union's General Data Protection Regulation ("GDPR") and various U.S. laws have been in place already, we can illuminate the experience of companies in complying with those laws. We also describe the costs of enforcement.

This paper proceeds as follows. Part I begins by briefly characterizing three of the major data protection regimes--the United States, the European Union, and China. Part II then describes the costs of private sector compliance with respect to each of these three regimes. Part III turns to the costs of public enforcement, again for these three different jurisdictions. Part IV concludes by drawing some lessons, focusing on developing countries.

I. Three Approaches to Data Privacy: EU, US, and China

We focus on three principal jurisdictions in this study, the European Union, the United States, and China. The rules in each of these jurisdictions have evolved significantly in recent years and continue to evolve so any account of their costs inevitably describes a moving target. In order to better

---

[7] While certain harms of data abuse are more readily calculable—such as those for identity theft—the harm from many data violations can be hard to assess. Thus, the full benefits of data protection are difficult to quantify. When describing the impact of a change to HIPAA rules in 2013, the Department of Health and Human Services noted, "We are not able to quantify the benefits of the rule due to lack of data and the impossibility of monetizing the value of individuals' privacy and dignity…." Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 FED. REG. 5566, 5567 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts 160 & 164). 78 FED. REG. 5567.

[8] UNCTAD Cyberlaw Tracker, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

[9] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L. J. 677 (2015).

understand the price of compliance and the costs of enforcement, we first summarize the major features of each regime below, drawing out some of the key approaches to compliance in these jurisdictions.

A. Compliance under the EU Data Privacy Regime

The GDPR requires that every entity processing personal data must have a legal basis to do so, such as consent or because it is necessary for the performance of a contract.[10] If that basis is consent, that consent must be "freely given, specific, informed and unambiguous."[11] Personal data must be processed lawfully, fairly, and transparently; collected for specified and legitimate purposes; adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; accurate; kept no longer than necessary for such purposes; and processed in a manner that ensures appropriate security.[12] It gives data subjects the rights to be informed, to access and rectify data, to be forgotten, to restrict processing, to data portability, and to object to certain processing of their data. The GDPR mandates that data controllers and processors institute privacy by design, seeking to implement data-protection principles in their products, taking into account both costs of implementation and risks for data subjects.[13] For data processing activities posing high risks to data subjects, the GDPR requires data controllers to carry out data protection impact assessments.[14] In addition, data controllers and processors may have to designate data protection officers when, for example, carrying out large-scale processing of special categories of data.[15] The GDPR goes beyond data privacy by, for example, giving each person the right to object to automated decision-making that produces legal effects on that person.

Because the GDPR adopts a risk-based approach, an organization's compliance obligations and related expenditures vary considerably depending on the risks posed by an organization's data collection or processing activities.[16] Data collection or processing that presents considerable risks to the rights and freedoms of data subjects by virtue of the nature, scope, context, and purpose of processing are high risk under the GDPR. Examples might include processing based on new technologies, and extensive automated decision-making with legal effects. As described above, such processing requires the implementation of procedures such as mandatory data protection impact assessments in which risks in processing are identified and safeguards presented, informing controllers of measures to be taken to mitigate and risk and, in certain cases, prior consultation with a Data Protection Authority before proceeding.[17] Furthermore, organizations are required to take the appropriate technical and organizational measures to properly safeguard personal data pursuant to the regulation's policy of data protection by design and default.[18]

---

[10] Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 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), art. 6, 2016 O.J. (L 119) 33 (EU) [hereinafter GDPR].

[11] *Id.* art. 4(11).

[12] *Id.* art. 5.

[13] *Id.* art. 25.

[14] *Id.* art. 35.

[15] *Id.* art. 37.

[16] European Commission, *The GDPR: New Opportunities, New Obligations* (2018).

[17] GDPR News, *What Is High Risk Under GDPR?* Compliance Junction, (2017); GDPR, art. 35-36.

[18] Council Directive 2016/679, art. 28, 2016 O.J. (L 119) 1, 2.

B. Compliance under the US Data Privacy Regime

The United States data privacy regime lacks a comprehensive law that regulates the collection and processing of personal data of U.S. residents by private parties. While there are constraints against government information collection through both the Federal Constitution and an extensive statutory framework regulating government use of personal data, there is no similar broad federal regulatory privacy law regulating private parties. Instead, the current data privacy framework arises out of a patchwork of federal and state laws, many of which are focused on a particular sector of the economy. By focusing the law on particular areas of concern, the United States has effectively chosen business freedom as a key principle in the area. Outside specified areas, the focus is limited to enforcing the privacy promises that businesses make to users, rather than on specific mandates setting out what businesses can and cannot do with data. Sectoral laws include the Health Insurance Portability and Accountability Act (HIPAA), covering the health industry, and the Gramm-Leach-Bliley Act (GLBA), covering the financial sector. In addition, the Federal Trade Commission Act (FTCA) gives the Federal Trade Commission broad authority to regulate data practices if they constitute "unfair or deceptive acts or practices in or affecting commerce."[19] Through the FTCA, the Federal Trade Commission serves as the nation's de facto privacy regulator, and its settlements create a kind of common law of privacy.[20]

HIPAA imposes an extensive set of privacy protections for personal health data gathered by covered entities, including hospitals, health care providers, and health insurers. Not only must health plans and health care providers give patients a written notice of their privacy practices, they must also "maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity and confidentiality of the information, and to protect against any reasonably anticipated threats."[21] These safeguards include designating a privacy official, training employees, and developing a system of sanctions for employees who violate the entity's policies.[22] HIPAA also mandates the Department of Health and Human Services (DHHS) to "adopt security standards that take into account the technical capabilities of record systems used to maintain health information, the costs of security measures, and the value of audit trails in computerized record."[23] There is extensive rule-making elaborating the statute.

The GLBA (also known as the Financial Modernization Act) regulates the use of nonpublic personal information by institutions or businesses engaged in financial activities such as banks, insurers, and brokerage firms. The GLBA empowers the Federal Trade Commission (FTC) to enforce the "obligations that establish standards for financial institutions relating to administrative, technical, and physical information safeguards."[24] Covered entities are obligated to protect any "personal information collected about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available."[25]

California's Consumer Privacy Act (CCPA), which went into effect at the beginning of 2020, will have significant impact, especially on larger enterprises. The nation's first comprehensive privacy law regulating commercial enterprise, the CCPA has a broad reach outside of California, covering all companies that do business in California and either (1) have an annual gross global revenue in excess of $25 million, (2) handle the personal information of at least 50,000 California residents, or (3) derive

---

[19] Fed. Trade Comm'n Act, 15 U.S.C. § 5 (2006)

[20] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2013).

[21] C. Stephen Redhead, RS20500, *Medical Records Privacy: Questions and Answers on the HIPAA Rule* 6 (Cong. Research Serv. 2004).

[22] *Id.*

[23] Pub. L. No. 104-191, tit. IV, §§ 261-264, 110 Stat. 1936 (1996).

[24] Pub. L. No. 106-102, tit. V, Subtitle A, 113 Stat. 1338 (1999).

[25] *Id.*

half or more of their revenue from selling consumers' personal information. Because many businesses in the United States (and elsewhere) meet this threshold, the CCPA effectively governs most multinational corporations (wherever they are based) that serve the United States.[26] The CCPA requires businesses to disclose the types and sources of personal data the business collects from customers, while granting California residents the right to access and delete personal information. The CCPA thus relies on a notice and consent model. The CCPA is principally enforced by California's Attorney General. These rights include the right to be notified about what personal information is collected and to opt out of the sale of that information.

C. Compliance under the Chinese Data Privacy Regime

China's data privacy regime is the newest of the three jurisdictions described here. It is best understood against the backdrop of China's development as a leading technological power that has simultaneously sought to maintain strong government control and public order. China's approach reflects a now nearly decade-old "national strategy to embrace 'big data.'"[27] With its data protection laws, China has embraced three goals simultaneously—to protect citizens' lawful interests, to protect networked information security, and to protect national security and public order.[28] A fourth goal, the promotion of China's technological advancement, has also been a key consideration in its implementation of data protection laws.

State security has been a focus of Chinese data policy from the start. The Golden Shield—nicknamed "the Great Firewall of China"—sought to ensure that the internet would not be used to disseminate information that might threaten public order and might even be used to create "an ennobling space where netizens complete their transformation into perfect citizens."[29] Typically, data protection policies are focused on the protection of the data of individuals and not at the promotion of state interests. However, data protection policies by their nature expand regulatory control over the activities of private companies and individuals, paving the way for China to operate its web and flow of data under the model of a cyber-sovereignty.[30] By focusing on state security, China prefers to implement regulations such as data localization laws to keep all its information within its borders, which enhances its ability to monitor and regulate information.[31]

In 2016, the Cyberspace Administration of China (CAC) issued Administrative Rules on Information Services via Mobile Internet Applications (the App Rules), seeking to directly regulate China's burgeoning app industry. These rules require app providers to obtain any necessary licenses or qualifications required of information services, make clear the nature and scope of data collection and use, and obtain consent from users before using location, address book, and camera features. App providers are also required to register the real names of their users, alongside information content

---

[26] See Anupam Chander, Margot Kaminski, & William McGeveran, *Catalyzing Privacy Law*, MINN. L. REV (forthcoming 2021).

[27] Jinting Deng, *Should the Common Law System Welcome Artificial Intelligence*: A Case Study of China's Same-Type Case Reference System, 3 GEO. L. TECH. REV. 223, 229 (2019). As Lu Chuanying, a scholar with the Shanghai Institutes for International Studies, describes, China has become a "leading data power (**数据大国**) on a global scale." Graham Webster & Rogier Creemers，*A Chinese Scholar Outlines Stakes for New 'Personal Information' and 'Data Security' Laws,* New America (May 28, 2020), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-scholar-outlines-stakes-new-personal-information-and-data-security-laws-translation/.

[28] Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, 8 PENN. ST. J.L. & INT'L AFF. 49, 69 (2020).

[29] Lorand Laskai, *Nailing Jello to a Wall*, in CONTROL 191 (ed. Jane Golley et al.).

[30] *Id.* at 197.

[31] Pernot-Leplay, *supra* note 28, at 104.

review.[32] The Cybersecurity Law also imposes real name registration obligations for information publishing and instant messaging services.[33] Being able to identify the user can be useful for the government in identifying lawbreakers, though human rights advocates have raised concerns about such requirements.

The cornerstone of China's data protection law can be found in the Cybersecurity Law enacted in 2017 by the Standing Committee of the National People's Congress. That law imposes numerous data protection obligations on "network operators," which are defined broadly to include "network owners, managers, and network service providers."[34] A central obligation is the requirement to obtain consent before collecting or sharing personal information.[35] While the laws themselves pose their requirements in very broad language, the government has provided guidance on their interpretation. In 2017, a technical committee supervised by the Cyberspace Administration of China and the Standardization Administration of China issued the National Standard of Information Security Technology – Personal Information Security Specification ("2018 Specification"), which became effective in 2018. While non-binding, the Specification has proved highly influential, establishing what have been described as a set of best practices related to data protection.[36] The government relies on this standard for enforcement actions.[37] The 2018 Specification often goes beyond the statutory text. For example, while the Cybersecurity Law requires only that companies "not gather personal information *unrelated* to the services they provide," the Specification goes further to limit collection only to information that is *necessary*.[38]

A revised Specification went into effect on October 1, 2020. This 2020 Specification requires affirmative (opt in) consent for processing sensitive personal information.[39] It also requires "fully informed" consent for the collection and use of biometric information. The 2020 Specification requires a data protection officer for organizations that process the personal information of more than one million people, organizations principally engaged in the processing of personal information and employing more than 200 individuals, or organizations that process sensitive personal information of more than 100,000 individuals. The 2020 Specification establishes new rules for companies that

---

[32] Norton Rose Fulbright, *China issues new rules to tighten regulation of Mobile Apps market*, Norton Rose Fulbright (July 2016), https://www.nortonrosefulbright.com/en/knowledge/publications/93003105/china-issues-new-rules-to-tighten-regulation-of-mobile-apps-market.

[33] Jones Day, *Implementing China's Cybersecurity Law* 2 (2017), https://www.jonesday.com/files/upload/Implementing%20Chinas%20Cybersecurity%20Law.pdf.

[34] Wangluo Anquan Fa（网络安全法）[Law on Cybersecurity] (promulgated by the Standing Comm. Nat'l People's Cong., November 7, 2016, effective June 1, 2017), art. 76 (3).

[35] *Id.* arts. 22, 41, & 42.

[36] Covington, *China Releases Draft Amendments to the Personal Information Protection Standard,* Data Privacy and Cybersecurity (February 11, 2019) https://www.cov.com/-/media/files/corporate/publications/2019/02/china_releases_draft_amendments_to_the_personal_information_protection_standard.pdf. Our interviewees confirmed that the Specifications were taken seriously, despite not having the force of law.

[37] Jenny (Jia) Sheng, Chunbin Xu, *China Publishes Best Practices for Protection of Perosnal Information* https://www.pillsburylaw.com/en/news-and-insights/china-publishes-best-practices-for-protection-of-personal-information.html.

[38] Cybersecurity Law, Art. 41 (emphasis added); Pernot-Leplay, *supra* note 28, at 94-95.

[39] Michelle Chan, Clarice Yue, Tiantian Ke, *China Cybersecurity Law Update: Two New National and Industry Standards: Personal Information Specification and Personal Financial Information Specification*, Bird & Bird (April 24, 2020), https://www.twobirds.com/en/news/articles/2020/china/china-cybersecurity-law-update-two-new-national-and-industry-standards; Hogan Lovells, *The dust has finally settled – the long journey of China's new Personal Information Security Specification* (April 2020), https://www.hoganlovells.com/en/publications/the-dust-has-finally-settled. An official English translation of the 2020 Specification is available here: https://www.tc260.org.cn/front/postDetail.html?id=20200918200432.

personalize information based on profiling, including targeted advertising.[40] The 2020 Specification provides detailed rules on the obligations of both personal information controllers and the third parties with which they share information. These include responsibilities for conducting security assessments of third parties, monitoring third parties, and disclosing to individuals that a third party will have access to their information.[41] The 2020 Specification also requires the information controller to take immediate action if it learns that a third party with which it has shared data has processed information inappropriately.[42]

The 2020 Specification adopts aspects of the GDPR model. The guidance, for example, requires companies that gather large amounts of personal information to appoint a data protection officer (though the Chinese specification is not technically binding). The guidance also imposes duties on data controllers with respect to third parties with whom they share information.

However, distinct differences remain. One of the architects of the 2018 Specification, Yuehong Hong, observes that these rules are "stricter than the U.S., but not as much as the EU."[43] For example, unlike the EU, where consent must be explicit, the Chinese interpretation of consent seems to permit implied consent, at least for non-sensitive personal information.[44] The right to port your data from one online service provider to another, while broad under the GDPR, is limited by the 2018 Specification only to an individual's basic information, as well as health, psychological, education and work information.[45] Yet at certain other points, the Chinese law, at least on its face, can be even more demanding than the EU law. For example, the Cybersecurity Law seems to make consent the exclusive basis for information collection, unlike EU law which allows a variety of bases for collecting personal information, including a category of "legitimate interests."[46] A draft proposal from the Cyberspace Administration of China would require network operators to inform "the local cyberspace administration when they collect important data or sensitive personal information;"[47] this would enhance the ability to regulate for security-related goals.

Security is also a key motivation for other aspects of the data regime. In comparison to the US's all-permissive approach to cross-border data flow and the EU's careful control on outward flows of personal data, China has moved towards highly restrictive policies to keep data within its own borders.[48] On June 13, 2019, China released a draft regulation on the outbound transfers of personal information, separating its treatment of "important data" and "personal information," which it had previously categorized under one umbrella.[49] With regards to the outbound transfer of personal information, the 2019 draft permits domestic network operators to enter into contractual agreements with foreign data receivers to allow for the transfer of personal data.[50] In order to transfer or access personal data outside the China, data controllers must (1) inform the data subject of the overseas transfer, (2) obtain express consent from the data subject, (3) store a copy of the data within China, (4) conduct a security assessment and file this with the local CAC, 5) establish data transfer agreements with overseas data receivers, 6) submit an annual report to the CAC on all related data transfers, 7) keep a record of all cross-border data transfers for a minimum of five years and 8) to appoint an officer

---

[40] Hogan Lovells, *supra* note 39, at 4.

[41] Sheng & Xu, *supra* note 32.

[42] Hogan Lovells, *supra* note 39, at 6.

[43] Pernot-Leplay, *supra* note 28, at 82, n. 150 and accompanying text.

[44] *Id.* at 84. The proposed amendments to the Standard also make provision for implied consent.

[45] *Id.* at 101.

[46] GDPR art. 6.

[47] Ken Dai & Jet Deng, *2019 China Data Protection Cybersecurity Annual Report* (Dentons 2020).

[48] Richard D. Taylor, *"Data Localization": The Internet in Balance*, 44 J. TELECOMM. POL'Y at 8 (2020).

[49] The Diplomat, *China's New Data Protection Scheme* (July 2019), https://thediplomat.com/2019/07/chinas-new-data-protection-scheme/.

[50] Taylor at 8.

to take care of compliance matters with CAC data security requirements.[51] While this technically allows cross-border data flows, the hurdles can be so high that many may find them to complex or expensive to manage.[52] The 2020 Draft Data Security Law addresses "important data," which must be kept strictly local. "Important data" relates to China's national, economic and public security as well as social stability.[53] The 2020 draft seeks to establish a system to monitor and warn of security data leaks, an emergency response system to handle security leak accidents, and a national security review system to investigate activities that may pose security threats.[54] Other guidelines such as the 2020 Personal Financial Information Protection Technical Specification issued by the People's Bank of China also govern the cross-border transfer of financial information and more specialized forms of data.[55] Neither the 2019 Personal Information Outbound Transfer Security Assessment Draft nor the 2020 Draft Data Security Law nor the 2020 Personal Financial Information Protection Technical Specification is yet binding law. While the 2017 Cybersecurity Law is binding, its laws are vaguely drafted and flexible in terms of interpretation.[56] Even though companies are not bound by law to comply with these guidelines, they are strongly encouraged to implement them to their best ability and treat these guidelines as the direction that the Chinese government intends to move.[57]

On July 2, 2020, the National People's Congress of China published a draft version of the new Data Security Law.[58] The draft law would clearly establish extraterritorial jurisdiction over companies outside China whose data usage harms Chinese national security. The draft also would establish that certain data with national security implications would be subject to export controls.

Practitioners suggested that a key cost of compliance was in setting up privacy management systems, including data mapping. One significant challenge was to change the internal culture to prioritize privacy.

II. Costs of Private Compliance

The cost for complying with privacy law varies dramatically—from the baker managing a relatively small database of her regular customers' orders to the 1,000-person company supplying information services to a variety of clients across multiple jurisdictions. In this Part, we summarize a variety of studies on the costs of compliance with respect to data privacy law in the EU and the United States.

The different studies paint vastly different portraits of costs. One study estimates mean expenditure for privacy compliance to be $1 million in 2018, the year the GDPR first went into effect, and $622,000 in 2019.[59] Another study, meanwhile, found an average focused on GDPR compliance

---

[51] DLA Piper, *Data Protection Laws of the World Handbook* 3 (2020), https://www.dlapiperdataprotection.com/index.html?t=about&c=AO at 5.

[52] *Cf.* Anupam Chander, *Is Data Localization a Solution for* Schrems II?, 23 J. INT'L EC. L. 771 (2020), at https://doi.org/10.1093/jiel/jgaa024 (arguing that hurdles for cross-border transfer out of the European Union post judicial rulings may be so burdensome as to effect a "soft data localization").

[53] Yan Luo & Zhijing Yu, *China Issued the Draft Data Security Law*, INSIDE PRIVACY (2020), https://www.insideprivacy.com/data-security/china-issued-the-draft-data-security-law/.

[54] *Id.*

[55] Norton Rose Fulbright, *PBOC Issues New Specification on Personal Financial Information* (March 2020), https://www.nortonrosefulbright.com/en/knowledge/publications/fcdc5f10/pboc-issues-new-specification-on-personal-financial-information.

[56] Pernot-Leplay, *supra* note 29, at 49, 74.

[57] *Id.*

[58] Nick Becket, Amanda Ge & Roxie Meng, *China Publishes Draft Data Security Law* (CMS, 2020).

[59] *See infra* note 69 and accompanying text.

budget of $13.2 million in 2018, rising to $13.6 million in 2019.[60] Estimates for compliance with U.S. privacy law are wide-ranging, but generally significantly lower.

The review below shows that compliance with the GDPR for large firms is quite expensive. Our survey respondents generally ranked the EU privacy regime to be the costliest of the three frameworks. They described the US as less expensive, whether for large or small firms, and compliance with Chinese privacy law as the least expensive, though that may be because of lack of awareness of the law. Among our respondents, cybersecurity costs seemed to be more significant with respect to Chinese and U.S. law compliance, than with EU law compliance. EU compliance costs seem to be heavily skewed towards personnel, both inhouse personnel and outside consultants.

As the wide ranges might suggest, the data is inherently limited. There is no consistent framework for analyzing the costs of compliance with data privacy laws. Every study seems to adopt its own methodology. One study, for example, breaks down costs as consisting of 1) the costs of granting access to data gathered on each consumer, 2) the costs of providing notice of privacy policies, 3) the costs of obtaining individual consent, 4) the costs of creating greater transparency, and 5) the costs of granting customers choice, including that of opting out or opting in to the database.[61] Another study meanwhile identifies the following components of data privacy costs: data protection and enforcement activities, incident response plans, compliance audits and assessments, policy development, communications & training, staff certification, redress activities, investments in specialized technologies to protect data assets such as threat intelligence, managed file transfer, identity and access governance, cyber analytics, data loss prevention, and encryption.[62] The studies are based on surveys of selected participants, which of course reflect who is invited to take them and who actually completes them.

Furthermore, any study of costs is necessarily incomplete. Privacy law also affects firms in ways that are difficult to quantify. If a firm decides not to offer a feature or decides not to enter a jurisdiction because of privacy law, the opportunity foregone is difficult to value. Little information is available on the costs of restructuring of operations by businesses to bring them into compliance.

We conducted a survey among privacy experts to seek to obtain information about the costs of compliance for private enterprises.[63] The survey was circulated to members of the International Association of Privacy Professionals, and was also circulated by leading privacy expert Daniel Solove to his LinkedIn network. We also emailed the survey to privacy lawyers we identified via web searches and through LinkedIn. The survey was open for responses from June 18 to August 3, 2020. The survey was posted to the web via Qualtrics and was available only to those that had the link. Various biases introduced by a web-based survey both suggest caution in relying on its results, and we do not rely on the survey results for our conclusions in this paper.

The questionnaire asked privacy professionals to indicate whether they worked at companies that largely collect data on those companies' own behalf, or companies that help other organizations manage their data. It tailored most of the remaining questions based on the answer to that initial query. The questions focused on the costs of complying with the privacy regimes of the three jurisdictions that are the focus of this study, the impact of those regimes on decisions by companies, and questions about cross-border data flows. To help provide consistency of responses, privacy professionals helping

---

[60] *See infra* note 69 and accompanying text.

[61] Christopher J. Robertson & Ravi Sarathy, *Strategic and Ethical Considerations in Managing Digital Privacy*, 46 J. Bus. Ethics. 111, 120 (2003).

[62] Ponemon Institute, *The True Cost of Compliance with Data Protection Regulations* 5 (Dec. 2017), https://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf.

[63] The complete survey and its results are posted here. https://drive.google.com/file/d/1CwzneOtePmmj0kZt7HBF-bxRkVfsORYc/view?usp=sharing.

other organizations manage data were requested to respond on behalf of two hypothetical clients: a small e-commerce firm with 100,000 user accounts and few overseas accounts; and a large business service provider with 100 million user accounts and operations in various jurisdictions. We received 51 responses to our survey from persons based in 17 different countries. The top countries among our respondents were the United States (43 percent), India (11 percent), Germany and UK (both 7 percent). Half of the respondents were consultants that help other organizations manage their data, while 36 percent were data controllers themselves. The bulk of the respondents (81%) had no foreign ownership, while 13 percent of the respondents had less than 50 percent foreign ownership and 6.38 percent of them had 50 percent or more foreign ownership. The percentage of respondents having more than 500 full-time employees was 41 percent, 17.39 percent of respondents have more than 50 fewer than 500 full-time employees, 19.57 percent of respondents have more than 10 and fewer than 50 full-time employees, and for 21.74 percent respondents, the number of full-time employees is between 1 and 10. Both the survey and the survey results are available online.

We also conducted interviews with a dozen leading experts across the world, in the United States, Europe, Africa, Asia, and Latin America. We promised confidentiality with respect to their identities so that they could advise us freely. We do not rely upon either our survey results or interviews as dispositive. The survey results and interviews have informed our study, but largely to serve as a check on our conclusions.

We highlight one especially costly component of data privacy because it is not limited to any one jurisdiction. Data breaches are expensive to respond to and highlight the need for proper cybersecurity to avoid such breaches. A global study conducted by the Ponemon Institute on behalf of computer hardware developer IBM analyzed breaches involving the loss or theft of customer or consumer records during July 2018 to April 2019.[64] Expenditures on activities and resources enabling the company to successfully detect the severity and reach of a breach had an average cost of $1.22 million.[65] An average of $0.21 million was expended on resources enabling organizations to notify regulators such as the GDPR's Supervisory Authorities, and affected data subjects of the relevant breach.[66] A Ponemon Institute survey found data breaches to be widespread among the companies surveyed: "About half of the respondents had GDPR data breaches that must be reported to regulators."[67] This was consistent across the world: "39% of US respondents, 45% of European respondents, 36% of Chinese respondents and 33% of Japanese respondents say they reported a personal data breach to a regulator."[68]

A. Compliance Costs for EU Data Protection Law

1. Overall Costs of GDPR Compliance

As indicated earlier, estimates for average annual compliance costs for the GDPR range widely, depending on the size of the company, the nature of its business, and other factors. For large firms, the estimates are routinely in the millions of dollars each year. A study conducted in 2019 by the International Association of Privacy Professionals (IAPP) in conjunction with Ernst & Young, a global professional service network, found mean privacy expenditures for the companies at which its survey respondents worked to be $1 million in 2018, the year the GDPR first went into effect, and $622,000

[64] IBM Security, *Cost of a Data Breach* (Ponemon Inst. (2019).

[65] *Id.*

[66] *Id.*

[67] Ponemon Institute, *Keeping Pace in the GDPR Race: A Global View of GDPR Progress in the United States, Europe, China and Japan* 2 (2019).

[68] *Id.*

in 2019. That study is not restricted to companies complying with the GDPR alone, but surveys companies across the world, including many in the United States. Research conducted by the Ponemon Institute in 2019 on behalf of international law firm McDermott Will & Emery (MW&E) focused on GDPR compliance found substantially higher figures: an average 2019 budget of $13.6 million for GDPR activities, a slight increase from $13.2 million in 2018.[69] The different results suggest the great variation in expenditures for compliance, depending on firm size, industry, types of activities, geography, perceived risks of operations, and risk tolerance. For the very large companies that make up the FTSE 100 stock index, estimates for GDPR compliance for 2018 range from an average of $84 million for banks, $26 million for technology and telecommunications firms, to $6 million for industrial goods and services firms.[70]

A high percentage of the costs (between a fifth and a half, depending on the study) are associated with hiring of privacy compliance personnel. Technology also accounts for a significant portion (between 12 to 17 percent, depending on study) of GDPR privacy expenses. Outside consultants and lawyers accounted for another 19 to 24 percent, again depending on the study. One study concluded that GDPR compliance required extensive person-hours in meetings; DataGrail estimates that the average company spent 2,100 hours in GDPR preparation meetings and that enterprises staffed with 1,000 or more employees could have spent over 9,000 hours in such meetings.[71]

Notably, despite these expenditures, most respondents (62% in the IAPP/EY study) believed their privacy budget was insufficient to meet their data protection obligations.[72]

The IAPP/EY study surveyed 370 respondents predominately composed of organizations headquartered in the U.S. (39%), European Union (33%), and United Kingdom (13%). Company size ranged from under 100 to over 75,000 employees and industry sectors represented included tech, finance, health care, government, and consulting services.[73] The salaries and benefits of an organization's privacy team constituted the majority of privacy spending, on average receiving $397,100, combined technology expenditures followed behind receiving an average mean privacy spend of $172,000.[74] Privacy expenditures are higher for organizations with more employees: organizations with 5,000 or fewer employees were estimated to have a mean privacy expenditure of $257,000 in 2019 whereas organizations with 75,000 or more employees had an estimated mean privacy expenditure of $1,883,200.[75]

Mean 2019 Estimated Privacy Spend Reported to IAPP by Employee Size, U.S. Dollars[76]

	<5K Employees	**5K-24.9K Employees**	**25K-74.9K Employees**	**75K + Employees**
Privacy Team Salaries	$170,700	$581,800	$744,200	$847,100
Privacy Team Technologies	$23,500	$47,100	$39,700	$115,600

[69] *Id.* at 27.

[70] Joseph Johnson, *GDPR Implementation Costs for FTSE100 Companies in the United Kingdom 2018 By Sector* (Statista 2018). Currency conversion from British pounds using XE.

[71] *Id.*

[72] *Id.* at 37.

[73] *Id.* at viii, xi.

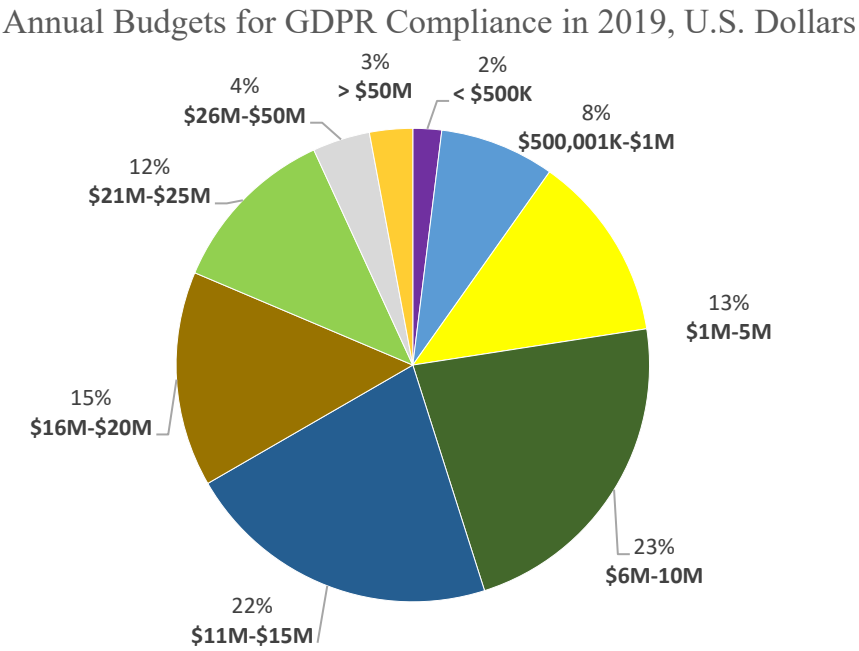
[74] *Id.* at 28.

[75] *Id.* at 30.

[76] *Id.*

Outside Privacy Team Technologies	$38,700	$30,500	$57,500	$814,200
Other Privacy Budget	$24,700	$84,500	$82,000	$106,200
TOTAL PRIVACY SPEND	$257,700	$743,800	$923,400	$1,883,200

The Ponemon Institute surveyed 1,263 organizations in 2019 on behalf of international law firm McDermott Will & Emery (MW&E). Respondents hailed from the U.S. (544), Europe (371), China (102), and Japan (246).[77] Organizations represented ranged from those with fewer than 500 to 75,000 employees and predominant industries were financial services (18%), industrial (13%), entertainment (11%) and the health sector (11%).[78] The survey found an average GDPR compliance budget of $13.6 million in fiscal year 2019.



[79]

2. Components of GDPR Compliance

[77] McDermott Will & Emery, *Keeping Pace in the GDPR Race: A Global View of GDPR Progress in the United States, Europe, China and Japan* (Ponemon Inst. 2019).

[78] *Id.* at 38.

[79] *Id.* at 62.

The studies shed light on the various components of the costs of compliance. Management services, personnel, and technologies continued to receive the greatest amount of funding, experiencing little to no changes in allocation since 2018.[80]

Distribution of Privacy Budget, 2018-2019			
Study	**Area of Budget**	**2019**	**2018**
MW&E, 2019 (McDermott Will & Emery)	Managed services	28%	28%
	Personnel	17%	18%
	Technologies	17%	17%
	Consultants	11%	10%
	Business process engineering	11%	10%
	Outside lawyers	9%	9%
	Training	7%	7%
IAPP-EY, 2019 (International Association of Privacy Professionals)	Salary & travel	50%	47%
	Technology & tools	12%	12%
	Outside counsel	10%	15%
	Internal training	9%	N/A
	Consulting services	8%	8%
	Professional development	7%	9%
	Gov. affairs	4%	3%
	Other	2%	4%

Statista attributes the large expenditure in banking to the high risk posed by their data processing activities as a bank data breach runs the risk of handing over the financial information and resources of data subjects, therefore requiring heavier investments in cybersecurity.[81]

Total Compliance Cost for FTSE 100 in Millions of U.S. Dollars		
Research Entity	**Industry**	**Cost of GDPR Compliance**
Statista, 2018	Banks	$93.8M
	Technology & Telecoms	$28.5M
	Energy & Utilities	$27.3M
	Retail	$21.4M
	Health care	$15.4M
	Travel & Leisure	$14.2M
	Financial Services	$11.3M

[80] *Id.* at 28

[81] Johnson, *supra* note 61.

	Media	$9.5M
	Industrial Goods & Services	$7.1M
Ponemon Institute, 2017	Financial Services	$30.9M
	Industrial	$29.4M
	Energy & Utilities	$24.8M
	Transportation	$24.3M
	Technology & Software	$23.6M
	Health care Pharmaceuticals	$19M $18.2M
	Consumer Products	$17.6M
	Communications	$16.7M
	Public Sector	$14.5M
	Retail	$11.5M
	Education & Research	$9.8M
	Media	$7.7M

Note: Figures have been converted from euros to U.S. dollars using XE's currency converter.

Salaries for privacy compliance personnel form a major part of privacy-related expenditures. A study by DataGrail surveyed 301 professionals involved in the GDPR decision-making process at companies with 50 or more employees in 2019 and found that 67% of companies engaged at least 25 employees when preparing for the GDPR, 44% of companies had at least 50 employees.[82] Findings from the IAPP's survey report that privacy staffing, like total privacy spending on GDPR compliance, reportedly leveled off in 2019, demonstrated by only 30% of organizations surveyed in 2019 expecting an increase in privacy staff, 66% expecting no changes, and 4% expecting a decrease.[83] An average mean of 7.1 employees work on privacy related matters full-time while a mean of 15.7 do so part-time.[84] Blended companies that engage in both business to business and business to consumer activities report the highest numbers in staffing along with privacy professional responsibilities, IAPP attributes the increase to the complexities such organizations face in role defining, negotiations, and contract-drafting due to their blurred role as data processors and controllers.[85]

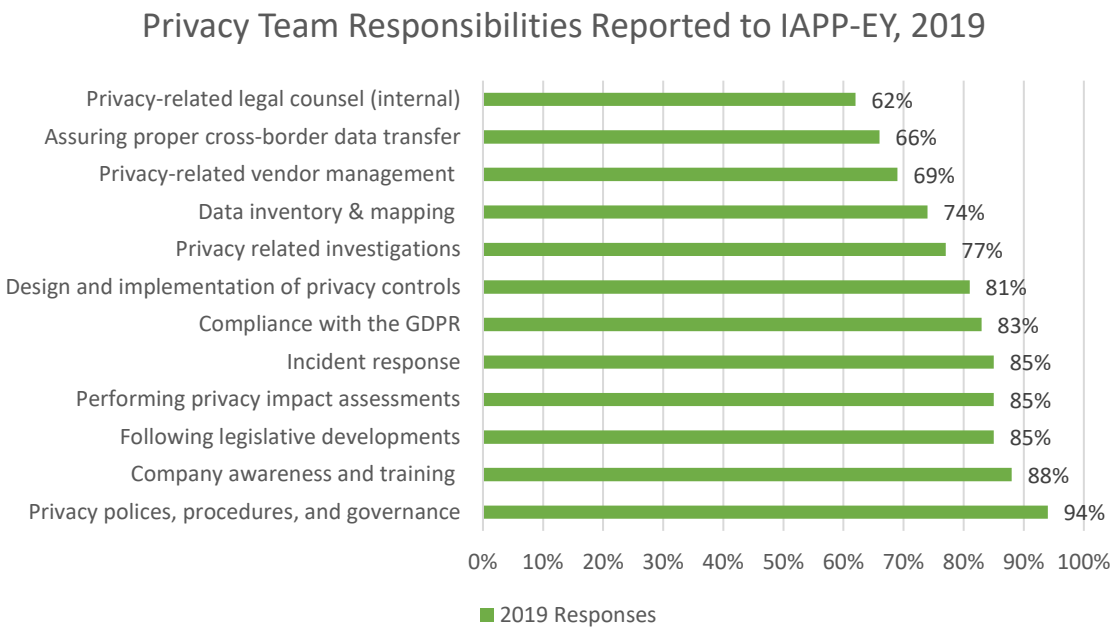
Research Entity	**Staff Related Expenditure**	**Cost**
IAPP-EY, 2019	Privacy team salaries and benefits (2019)	$397,100 (avg.)

[82] DataGrail, *The Age of Privacy: The Cost of Continuous Compliance* (DataGrail 2020).
[83] J. Trevor Hughes & Angela Saverice-Rohan, *Annual Privacy Governance Report* (IAPP-EY 2019).
[84] *Id.*
[85] *Id.* at xiv.

(Respondents: 370 privacy professionals from the IAPP database located in U.S. and E.U.)	Salary and travel (2018) Salary and travel (2019)	47% of privacy budget 50% of privacy budget
Paul Hastings, 2017 (Respondents: 100 FTSE 350 & 100 Fortune 500 companies)	Additional staff (U.K.)	$263,600 – $524,700
	Additional staff (U.S.)	$501,000 - $1M

Note: Data figures have been converted from Euros to U.S. Dollar using XE's currency converter and rounded.

Data from MW&E's study reported that almost half of the organizations represented (48%) are either in the process or expecting to hire an average of almost four additional employees to provide ongoing assistance with the GDPR.[86] Despite the expected increase for some, 38% of organizations in the research group believe their organization lacks the human resources to fulfill their obligations and sustain GDPR compliance in 2019.[87]



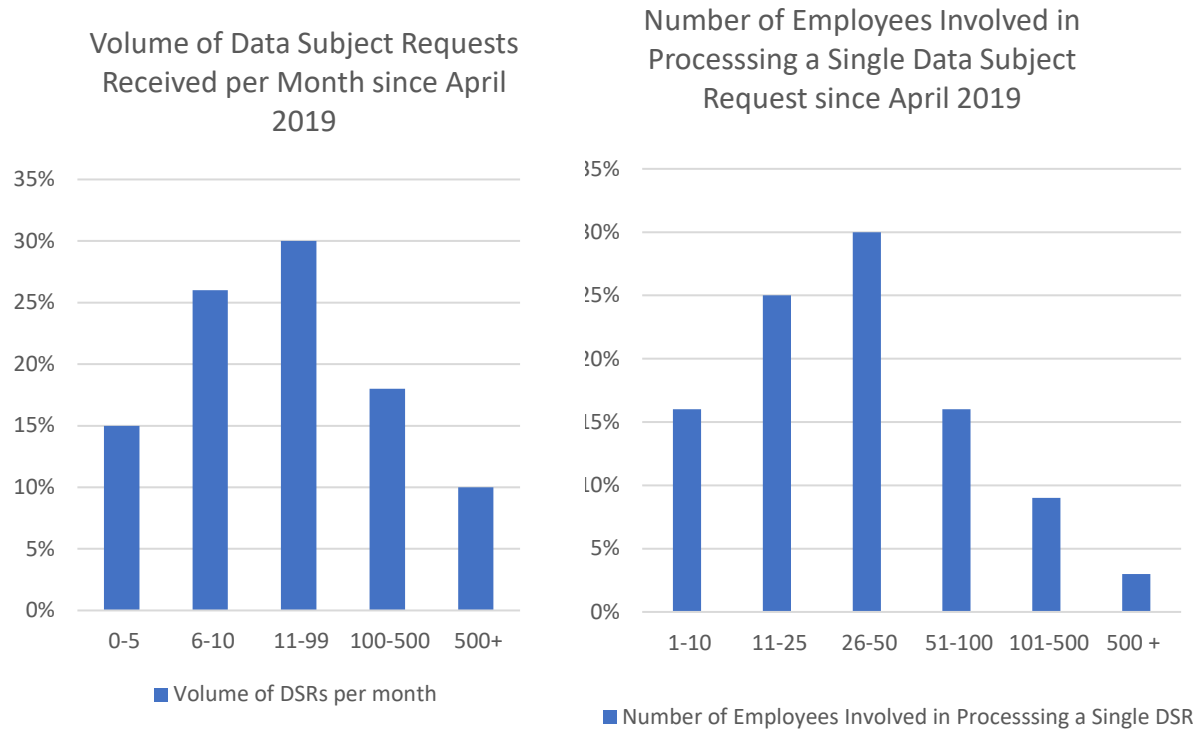
[88]

The GDPR permits individuals to request the data that companies hold on them, a process that requires an inventory of the data that companies hold, and can require configuration of their databases. According to DataGrail's survey findings, 58% of companies had received 11 or more data subject requests per month since the GDPR's implementation and the survey's closing in April 2019,

[86] McDermott Will & Emery, *supra* note 68.
[87] *Id.* at 25.
[88] Hughes & Saverice-Rohan, *supra* note 74.

and 28% received 100 or more per month.[89] A reported 58% of companies had at least 26 employees processing a single data subject request in 2018; this is likely attributable to the multi-step process of registering the request, verifying the requester's identity, and locating the data on multiple systems, an onerous task for organizations many of which log such information on spreadsheets. [90]

Operational Cost of Managing Data Subject Requests[91]



The manual handling of data subject requests has placed a strain on some organizations due to the time and effort involved in servicing the requests within the required one-month window. Duties imposed by a data subject request range from locating, compiling, and providing a data subject with all the information an organization has stored on a data subject, free of charge, commonly known as "the right to access,"[92] to locating and deleting all the information stored on a data subject, "the right to be forgotten."[93] The challenges posed by data subject requests were echoed by the IAPP's study in which 56% of the 370 organizations surveyed reported "locating unstructured personal data" as "difficult."[94]

The operational costs that data subject requests impose on an organization appear to be related to the organization's location, business model, size, and revenue.[95] Findings from the IAPP report suggest that the firms most likely to receive data subject requests have one or more of the following variables: headquarters in Europe, a blended business model in which both data controlling and

[89] DataGrail, *supra* note 73.
[90] *Id.* at 3, 8.
[91] DataGrail, *supra* note 73.
[92] Council Directive 2016/679, art. 23, 2016 O.J. (L 119) 1, 2.
[93] *Id.*, art. 25, 2016 O.J. (L 119) 1, 2.
[94] Hughes & Saverice-Rohan, *supra* note 74.
[95] *Id.*

processing were present, an excess of 25,000 employees and/or revenue exceeding $25 billion.[96] IAPP respondents which received higher levels of data subject requests reported experiencing less difficulty managing requests than respondents who received fewer.[97] The IAPP attributes this relationship to the increased investments many organizations make toward automating the process of locating a data subject's information when facing high quantities of requests, thereby decreasing the amount of time and staff needed to complete the task.[98]

Though an organization is only required to hire a Data Protection Officer when either (1) the processing of personal data is a core business activity, (2) the activity involves "sensitive" information, or (3) the processing is performed routinely on a large scale, studies suggest many organizations have heeded the GDPR's encouragement to appoint a Data Protection Officer even when not required. An overwhelming 92% of MW&E's 1,263 respondents[99] and a three-fourth of the IAPP's 370 respondents[100] appointed Data Protection Officers despite both surveys including a wide variety of organizations in which the criteria mandating an appointment were unmet. Most organizations have appointed only one Data Protection Officer, though 18% of organizations have expended resources on appointing multiple.[101] Although a Data Protection Officer's compensation varies by region and experience, officers were reported to have a global salary range between $71,000 and $354,000 in 2018.[102]

MW&E's 2019 study found that 46% of respondents had hired outside counsel for GDPR compliance.[103] The survey found that 68% of organizations hired outside counsel to conduct data protection impact assessments, a time and labor extensive procedure performed whenever a new processing activity is proposed and required of organizations engaging in high-risk processing.[104] Contacting data protection agencies (56%), overall risk mitigation (54%), establishing a consent mechanism for processing (49%), and response to a data subject's "right to be forgotten" (49%) followed behind as common reasons for enlisting outside assistance.[105] Approximately 34% of respondents sought outside counsel for assistance with international data transfers. The invalidation of the EU-U.S. Privacy Shield by the Court of Justice of the European Union in 2020, a data transfer mechanism utilized by 60% of IAPP respondents, will undoubtedly result in further legal expenditures in the area in 2020.[106]

Percent of Budget Allocated on Outside Counsel & Consulting Services			
Research Entity	**Outside Counsel and/or Consulting Service**	**2019**	**2018**
Ponemon Institute (2019)	Consultants	11%	10%
	Outside Lawyers	9%	9%
IAPP-EY (2019)	Outside Counsel	10%	15%

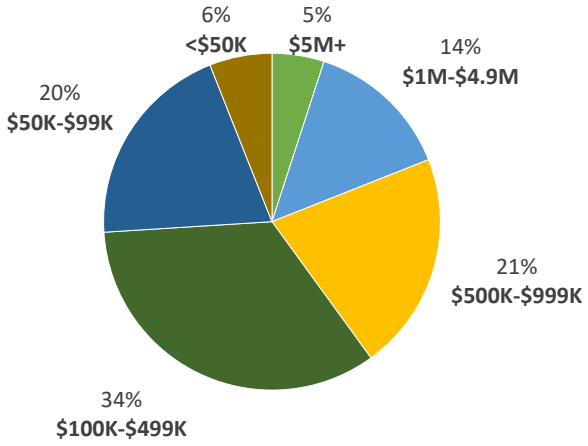
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] McDermott Will & Emery, *supra* note 68.
[100] Hughes & Saverice-Rohan, *supra* note 74.
[101] *Id.*
[102] Oliver Smith, *The GDPR Racket: Who's Making Money From This $9BM Business Shakedown*, Forbes (2018).
[103] McDermott Will & Emery, *supra* note 68, at 23.
[104] *Id.*
[105] McDermott Will & Emery, *supra* note 68.
[106] Hughes & Saverice-Rohan, *supra* note 74; *See also* Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, 2020 E.C.R. I-0000.

	Consulting Services	8%	8%

Expenditures on third parties hired to process an organization's personal data have become commonplace, with 90% of the IAPP's respondents reporting that their processing was outsourced.[107] The GDPR mandates that personal data should be outsourced to third parties for processing only when those processors provide sufficient guarantees that processing will occur in accordance with the GDPR through a written contract.[108] Data controllers remain responsible for non-compliance by the processors with which they share data. The IAPP reports that only 26% of respondents conducted on-site audits to ensure GDPR compliance, with several respondents observing that doing so was labor-intensive and potentially cost-prohibitive. An overwhelming majority of respondents (94%) rely on the assurances in the contract instead, with 57% of respondents supplementing the contact with questionnaires provided to processors to verify GDPR compliance.[109]

The GDPR does not outline specific technologies that organizations should use, though the use of encryption and pseudonymization are encouraged and required whenever feasible.[110] The IAPP found an average of $172,000 spent on technology expenditures.[111] Of the 301 privacy professionals involved in the decision-making process of their respective organizations, 58% of those surveyed by DataGrail purchased commercial technology solutions in pursuit of GDPR compliance and 57% invested in developing internal technology solutions.[112] Showing similar results from a surveyed pool of 370 privacy professionals, 46% of the IAPPs respondents invested in new technologies or services in preparation for GDPR compliance.[113]

Company Spending on Consulting Services and/or Technology in Preparation for GDPR Compliance[114]



[107] *Id.*
[108] Council Directive 2016/679, art. 28, 2016 O.J. (L 119) 1, 2.
[109] Hughes & Saverice-Rohan, *supra* note 74, at xv.
[110] *Id.* art. 32, 2016 O.J. (L 119) 1, 2.
[111] Hughes & Saverice-Rohan, *supra* note 74. .
[112] DataGrail, *supra* note 73.
[113] Hughes & Saverice-Rohan, *supra* note 74.
[114] DataGrail, *supra* note 73.

Manual v. Automation: Methods Used by Organizations in GDPR Compliance[115]	
Tools used for data inventory and mapping	60% email, spreadsheets, in-person communication (manual)
	31% commercial software tool designed for data inventory/mapping
	21% Data Loss Prevention (DLP) technology
	20% GRC software customized in-house for inventory/mapping
	8% Outsource data inventory/mapping to external consultants/law firms
	4% Don't know
Method for handling Data Subject Requests	64% Entirely manual
	25% Partially automated
	7% Still being designed
	2% Haven't yet addressed
	1% Automated

Of the 1,263 organizations surveyed by MW&E, 31% of respondents purchased insurance covering cyber risks. Of those insured, 43% had insurance coverage for GDPR fines and penalties.[116] Expenditures on cybersecurity insurance vary by region with 19% of Chinese respondents, 35% of U.S. respondents, 29% of European respondents, and 31% of Japanese respondents reporting an insurance purchase.[117] Data breach disclosure requirements continue to be a challenge for many organizations with only 18% of MW&E's respondents confident in their ability to notify a data protection authority within 72 hours of becoming aware of the incident, as required by the GDPR.[118] The study suggests that many organizations need further expenditures on external cybersecurity services that would enable organizations to identify cyberattacks early on and provide data protection authorities the necessary forensic evidence within the mandated window of time.[119]

The GDPR permits regulators to fine organizations up to €20 million or 4% of an organization's global annual turnover, whichever is higher, in cases of noncompliance with the GDPR. For the largest companies, this could result in fines in the millions or even billions of dollars. When a personal data breach occurs, an organization must provide notification describing, at minimum, (1) the nature of the breach, (2) its potential consequences, and (3) the measures the organization proposes to mitigate any harm.[120] As of November 30, 2020, there have been approximately 460 instances where fines have been imposed on organizations under the GDPR.[121]

[115] Hughes & Saverice-Rohan, *supra* note 74.

[116] McDermott Will & Emery, *supra* note 68.

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] Council Directive 2016/679, art. 33, 2016 O.J. (L 119) 1, 2. No such notification is required if the data breach is unlikely to present a risk to the rights and liberties of data subjects or seasonable notification is rendered unfeasible by circumstance.

[121] CMS Law, *GDPR Enforcement Tracker* (2020), https://www.enforcementtracker.com.

B. Compliance Costs for US Privacy Law

Because of the sectoral nature of U.S. privacy law, we examine studies detailing the costs of compliance with respect to industries, particularly health and finance.

1. HIPAA Compliance Costs

Studies over the last two decades have estimated that the health industry, as a whole, expends billions of dollars on HIPAA compliance initiatives. In 2003, health care consulting companies estimated the cost for compliance to total $25 billion to $43 billion in the first five years.[122] The Department of Health and Human Services, however, estimated that industry-wide implementation would cost $3.2 billion in HIPAA's first year and $17.6 billion for the first ten years.[123] In 2003, the research firm Gartner Group estimated that the health care industry would spend between $3.8 billion and $38 billion in pursuit of HIPAA compliance from 2003 to 2008.[124] For individual health care providers, the cost could total millions of dollars over time. In 2002, Baylor University Medical Center budgeted $7.5 million over the course of five years to account for HIPAA implementation. Texas Health Resources trained 22,000 workers before an April 14, 2003 deadline, and expected to spend more than $10 million to comply with the law.[125] Peter Swire, then Chief Privacy Counsel for the Clinton Administration, projected that HIPAA's Privacy Rule would cost $6.25 per year for every insured American.[126]

Cost of HIPAA Compliance for Entire Industry[127]

Research Entity	**Affected Respondents**	**Estimated Cost of Compliance**
Healthcare Consulting Companies (2003)	Health care providers (covered entities)	$25-43 billion (first 5 years)
Department of Health and Human Services (2002)	Health care providers (covered entities)	$3.2 billion (first year) $17.6 billion (first 10 years)
Gartner Group (2003)[128]	Entire health care industry	$3.8 - $38 billion (2003-2008)

In 2011, after certain HIPAA modifications, the Department of Health and Human Services (DHHS) conducted a study to estimate the additional cost of compliance imposed by the

[122] Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 Admin. L. Rev. 85, 132 (2002).

[123] *Id.*

[124] Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 Admin. L. Rev. 85, 132 (2002).

[125] Principle Logic, LLC, *HIPAA Cost Considerations* 24 (Oct. 11, 2003).

[126] *Id.*

[127] *Id.*

[128] Rebecca Herold & Kevin Beaver, *The Practical Guide to HIPAA Privacy and Security Compliance* (Auerbach Publ'n 2014).

modifications.[129] DHHS surveyed "covered entities," which include all health plans, health care clearinghouses and health care providers. The DHHS estimated the additional costs incurred to be between $114 million and $225.4 million in the first year of implementation and approximately $14.5 million annually thereafter.[130] These costs include: (i) costs to HIPAA covered entities to revise and distribute updated notices of privacy practices; (ii) costs to HIPAA covered entities to comply with the requirements of breach notification; (iii) costs to business associates to ensure their subcontracts are complying with business associate agreement requirements; and (iv) costs to business associates to fully comply with HIPAA's security rule.[131]

Legislation	**Estimating Entity**	**Affected Respondents**	**Cost of Compliance (US$/year)**	**Cost of Compliance Components**
Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules	Department of Health and Human Services (2013)[132]	700,000 covered entities.	$55.9 million	Notices of Privacy Practices
		19,000 covered entities.	$14.5 million	Breach Notification Requirements
		250,000–500,000 business associates of covered entities	$21–42 million	Business Associate Agreements
		200,000–400,000 business associates of covered entities	$22.6–113 million	Security Rule Compliance by Business Associates
	Total Costs		$114–225.4 million (first year) $14.5 million (annually after)	

The following tables break down the estimated costs expended by covered entities and the business associates of covered entities in order to comply with the modified provisions of HIPAA, according to the DHHS study.[133]

[129] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts 160 & 164).

[130] *Id.* at 5567.

[131] *Id.*

[132] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts 160 & 164).

[133] *Id.* at 5676.

Annual Compliance Costs for Notice of Privacy Practices			
Legislation	**Affected Respondents**	**Cost of Compliance (US$/year)**	**Cost of Compliance Components**
HIPAA	698,238 covered entities (providers, health insurers and third-party administrators)	$20 million	Drafting privacy notices
		$22.4 million	Printing privacy notices
		$13.5 million	Mailing privacy notices
Total Costs		$55.9 million/year	

Annual Compliance Costs for Breach Notification
(Total for 698,238 Covered Entities)[134]

Cost of Compliance (US$/year)	Cost of Compliance Components
$3,467,122	E-mail and 1st Class Mail • Includes the cost to compose and document notice, the hours and cost to prepare mailing, as well as necessary postage and supplies
$571,200	Substitute Notices: Media Notice
$1,816,379	Substitute Notices: Toll-free Number • Includes monthly and direct charges to the line, labor costs, and costs to individuals
$2,052,665	Imputed cost to affected individuals who call the toll-free line
$15,420	Notice to Media of Breach: Over 500
$15,420	Report to the Secretary: 500 or More
$5,277,456	Investigation Costs: Under 500
$837,500	Investigation Costs: 500 or More

[134] *Id.* at 5671.

$422,438	Annual Report to the Secretary: Under 500
Total Costs	$14,475,600/year

2. GLBA Compliance Costs

Robert Hahn and Anne Layne-Farrar's 2002 study detailed the industry-wide cost of compliance with the Gramm-Leach-Bliley Act (GLBA). The study found that banking, insurance and securities companies may, altogether, spend around $2- billion to $5 billion on printing costs alone to comply with the regulation's privacy policy notifications. In 2016, nearly 15 years after Hahn and Farrar's study in 2002, amendments to the GLBA created exceptions to the annual privacy notice requirements.[135] In response, the Bureau of Consumer Financial Protection calculated the decreased cost of privacy notice procedures yielded from the modifications and found a $3 million reduction in costs incurred per institution.

Legislation	**Estimating Entity**	**Affected Respondents**	**Cost of Compliance Components**	**Cost of Compliance (US$/year)**
GLBA[136]	Fred H. Cate and FleetBoston Financial Corporation	Banking, insurance and securities companies (surveyed 40,000 financial institutions)	Printing costs for all privacy policy notifications[137]	$2-5 billion in the entire financial industry
			1. Drafting policy 2. Consulting lawyers 3. Hiring part-time and full-time IT employees 4. Hiring a Chief Privacy Officer	Not estimated
Amendments to the GLBA[138]	Bureau of Consumer Financial Protection	Banks, credit unions and non-depository financial institutions.	Cost of annual privacy notice	$12 million (pre-amendment) - $3 million (savings from amendment) = $9 million per institution

[135] Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act, 83 Fed. Reg. 40945 (Aug. 17, 2018) (to be codified at 12 C.F.R pt. 1016).

[136] Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 Admin. L. Rev. 85, 145 (2002).

[137] Fred H. Cate, The Privacy Paradox (Jan. 26, 2001) *(observing that "*[a]pproximately 40,000 financial institutions will be sending as many as 2.5 billion notices to their various customers by June 12, 2001" to comply with the Gramm-Leach-Bliley Act.)

[138] *Id.*, 83 Fed. Reg. 40956 (Aug. 17, 2018) (to be codified at 12 C.F.R pt. 1016).

		(surveyed 19 banks with assets over $100 billion + 106 additional banks selected through random sampling)		→ Reduction in burden (per bank) = $3 million/year. → Reduction in burden (per non-depository financial institution) = $231,000/year

3. COPPA Compliance Costs

Compliance with the Children's Online Privacy Protection Rule (COPPA) appears to be less costly than those associated with HIPAA or GLBA. In 2000, the House of Representative's Committee on Commerce estimated the cost of compliance with COPPA to range from $115,000 to $290,000 per year for a mid-sized children's website, depending on the nature of the site.[139] The House Committee broke down the costs as indicated in the figure below.[140]

Breakdown of Estimated Costs in Year 2000 of COPPA Compliance for a Website

Activities	**Cost**
Legal (audits, construction of private practices and policy)	$10,000 - 15,000 (one time)
Engineering costs to make the site compliant	$35,000 (one time)
Professional chat moderators (price differs depending on training, hours of operation, and organization)	$25,000 - $10,000 per month
Personnel overseeing offline consent, responding to parents' questions, reviewing phone consents, and reviewing permission forms	$35,000 - $60,000 per one person per year in charge of these activities
Personnel overseeing compliance, database security, responding to verification and access requests	$35,000 - $60,000 per one person per year in charge of these activities

Some companies have sought to avoid COPPA altogether by excluding children under age 13 from their consumer base instead of undertaking measures to comply with the legislation.

---

[139] *Recent Developments in Privacy Protections for Consumers*, One Hundred Sixth Cong. 83 (2000) (Hearing Before Subcommittee on Telecommunications, Trade, and Consumer Protection of the Committee on Commerce, House of Representatives).

[140] In 2013, definitions of terms such as "personal information" and "operator" were expanded and the requirements for notice, parental consent, confidentiality, security, and data retention and deletion were updated. According to an estimate by the Federal Trade Commission, existing businesses could spend more than $6,200 per year to comply with the new rules, while new companies could face up to $18,670 per year. Manatt Phelps & Phillips LLP, Have Coppa Changes Resulted in Less Content, Higher Costs? (2013), https://www.lexology.com/library/detail.aspx?g=0b6d68a9-5d17-4d52-9b30-54d356ddb08a.

C. Compliance in China

We were unable to locate studies on the costs of private sector compliance with China's data privacy regime.

In an experiment conducted by Tianshu Sun and his colleagues on Alibaba's platform in China, researchers found that when algorithmic recommendations were prohibited by privacy law (because they often rely on customer profiles), customer engagement and actual marketplace transactions significantly decreased.[141] Though the study focused on a Chinese platform, the findings imply one type of cost precipitated by privacy laws.

Civil and criminal sanctions, as well as administrative penalties, are available as consequences for violations of cybersecurity laws. Remedies can include warnings, orders to rectify, fines, compensation to victims, and even prison sentences.[142] In comparison to the GDPR, which permits fines of up to 2% of a company's global annual revenue, an amount that can be in the billions of dollars for large companies, the fines available under the Chinese law are relatively low—allowing a maximum fine of approximately RMB 1,000,000 (about $141,000) under the Cybersecurity Law. Authorities may seek sanctions against responsible personnel, and may also revoke the license to operate, resulting in the shutdown of an app or website entirely—a remedy even more serious than financial penalties.

Over the last two years, the Chinese authorities have acted against websites and apps that violated the nation's data protection laws. Authorities have sought to audit the collection and use of personal information by mobile apps, evaluating more than 1,000 apps for data practices, and requiring subsequent changes from many of them.[143] In 2018 and 2019, the Cyberspace Administration of China conducted an enforcement action against mobile apps to target pornography, gambling, malicious programs, and other disfavored content, reportedly shutting down approximately 33,638 apps which were found to possess illicit content.[144]

While data protection practices have garnered increased attention, much of the enforcement related to the digital economy thus far seems targeted at issues of public order. Regulating data protection practices may be construed as part of a broader effort to ensure control, through audits, of information circulated online, and thus as part of a national security effort.[145]

In 2019, China's National Information Security Standardization Technical Committee proposed revisions to the 2018 Specification, calling for companies that either (a) employ more than 200 people to process personal data or (b) process more than 1 million people's data over the span of 12 months, to appoint a person or office to oversee data protection.[146] Nevertheless, prior to the implementation of this requirement, the private sector's costs of compliance with the Cybersecurity Law were commonly defined by litigation costs.[147] For instance, tech companies such as WeChat, ByteDance and Tencent have previously sought to seek and prevent access to protected information by initiating civil disputes against their competitors in court.[148] In the past few years, ordinary citizens are increasingly taking advantage of this system to fight tech companies in pursuit of their own privacy rights.[149] Private costs of compliance can also be inferred from the Cybersecurity Law penalty system.

---

[141] Tianshu Sun, Zhe Yuan, Chunxiao Li, Kaifu Zhang, Jun Xu. 2019. *The Value of Personal Data in Internet Commerce: A High-stake Field Experiment on Data Regulation Policy*, SSRN Working Paper: Available at https://ssrn.com/abstract=3566758.

[142] DLA Piper, *supra* note 46, at 6.

[143] Dai & Deng , *supra* note 42, at 15.

[144] *Id.* at 16.

[145] Anupam Chander, *Googling Freedom*, 99 Cal. L. Rev. 47 (2010).

[146] Gil Zhang & Kate Yin, More Updates on the Chinese Data Protection Regime in 2019 (IAPP 2019).

[147] Dai & Deng, *supra* note 42 at 20.

[148] *Id.* at 3, 20-21.

[149] *Id.* at 21.

When companies fail to comply with the 2017 Cybersecurity Law, they are subject to 100,000 to 1,000,000 RMB (US$14,351 - $143,517) in fines.[150]

While the Cybersecurity Law, like the GDPR and to a certain degree the CCPA, applies to businesses and organizations in all industries, several sectors in the private sector have additional requirements regarding data protection and privacy.[151] Within the life sciences industry, China focuses most of its regulation efforts on localizing health care data and scientific research to protect against illicit cross-border transfers of data through legislation such as the Measures for the Management of Scientific Data and the Measures for the Management of Population Health Information.[152] According to Dentons, health care companies comply with the Cybersecurity Law by categorizing its circulated data, developing protection policies, and localizing servers storing this information.[153]

The People's Bank of China led regulatory efforts within the financial industry by publishing the Implementation Measures for Protecting Financial Consumers' Rights and Interests in December of 2019 and bringing into effect the Personal Financial Information Protection Technical Specification in February, 2020.[154] The government published the National Standards on Information Security Technology in March 2020 and they came into force in October 2020.[155] These regulations focus on protecting consumer financial information and aim to crack down on illegal crawler technology.[156] Companies in the financial industry are advised to construct a sound security system by encrypting data and ensuring adequate access controls, and are encouraged to justify the purpose, method and scope of the data collection.[157]

The Information Security Technology Personal Information Security Specification governs the E-Commerce industry, including regulations on how companies may obtain consent from customers and store their respective data.[158] Online retail stores are advised to require clear and affirmative consent from customers when collecting personal information, anonymize personal data, have clearly written contracts with suppliers, and prepare a data breach response plan.[159]

III. Costs of Public Enforcement

How much does it cost to enforce privacy regulations? We examine this question by analyzing the budgets of the agencies tasked with enforcing data privacy law in Europe, the United States, and China.

This section aims to identify the financial and employee resources available to the regulators and compare it with the enforcement actions undertaken by the respective regulators. Both the EU and the US agencies regularly publish this information on an annual basis. While China has in the last two years actively enforced data security and privacy rules, we could not locate information on the budgets for the various Chinese regulators engaged with data privacy enforcement.

China's data protection regime is the newest of the three major global privacy regimes. Unlike the GDPR and the US regulations, the Chinese data protection regime does not have a single regulator.

---

[150] Kpmg China, Wanglu Anquanfa Gailan (网路安全法概览) [An Overview of China's Cybersecurity Law] at 6 (2017).

[151] Dai & Deng, *supra* note 42, at 23.

[152] *Id.* at 24-25.

[153] *Id.* at 25.

[154] Bird & Bird, *supra* note 34.

[155] *Id.*

[156] Dai & Deng, *supra* note 42, at 26.

[157] *Id.* at 27.

[158] *Id.* at 28-29.

[159] *Id.* at 29.

Instead, the Cyberspace Administration of China seems to be the primary regulator, and agencies like the Ministry of Industry and Information Technology, the Ministry of Public Security, the State Administration for Market Regulation, and the Ministry of Science and Technology are also vested with significant regulatory and enforcement roles. Budgets for data protection enforcement were not readily available, so we limit our discussion to describing enforcement activities.

This is a fast-changing area, and any snapshot will not capture the full dynamics at play. While the GDPR builds upon an earlier privacy regime, all of the privacy regimes in these three jurisdictions have undergone dramatic changes in the last two years. Indeed, the CCPA just went into effect this year, and has yet to see its first enforcement action. What this review makes clear is that budgets for enforcement have not kept up with either the regulations or the scope of the digital economy.

A. Enforcement in the EU

1. Overview

On average, the then-28 European Union member states allocated €12.1 million to each of their data protection authorities in 2020.[160] At the high end, Germany allocated €85.7 million among both its federal and state data protection authorities, while Cyprus, Malta, and Estonia, allocated just €0.5 million, €0.6 million, and €0.8 million for the latest year available.[161]

The GDPR requires each EU Member States to establish Data Protection Authorities (DPA) with sufficient financial resources for their operation.[162] The DPAs enforce the GDPR, and also raise awareness, provide guidance, handle complaints, and conduct investigations. The GDPR also imposes a duty of cooperation on Member States.[163] The GDPR hoped to create a one-stop shop enforcement mechanism, charging the supervisory authority of the "main establishment" of the controller or processor as the "lead supervisory authority" for the cross-border processing activities of that controller or processor.[164] Secondary "concerned authorities" may also assist in the investigation.[165]

Budgets allocated to DPAs are generally increasing, although at significantly lower rates than the one time jump observed between 2017 and 2018, the latter being the year when the GDPR went into effect.[166] Twenty-one of the 30 DPAs surveyed by the European Data Protection Board (EDPB)[167] reported dissatisfaction with their level of resourcing.[168] This dissatisfaction stems from a combination of the following: (1) significant increases in data privacy complaints, especially those that implicate big tech firms or carry cross-border components, (2) the complex system in which cross-border complaints are handled; and (3) insufficient resources to match complaint growth.

2. National Enforcement

Most European governments spend less than a euro per citizen per year on their data protection authority. Many supervisory authorities complain of insufficient funding. Despite such

---

[160] This excludes Cyprus, for which the 2020 budget allocation was not reported.

[161] Johnny Ryan & Alan Toner, *Europe's Governments are failing the GDPR*, 2020 (vacancies included in count and full-time equivalents are rounded; data on Austria's tech specialists unavailable).

[162] Council Directive 2016/679, art. 52, 2016 O.J. (L 119) 1, 2.

[163] *Id.* art. 31.

[164] GDPR, art. 56.

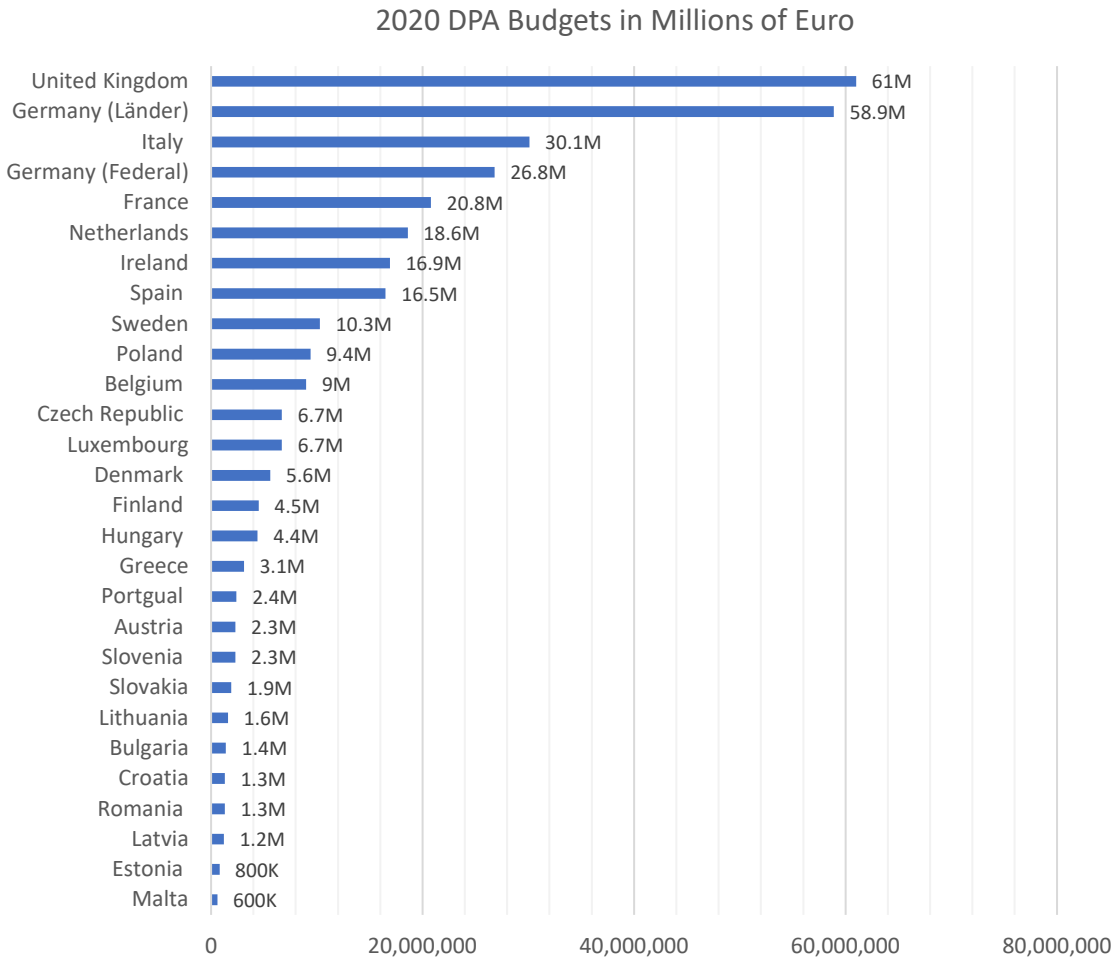
[165] *Id.* art. 4(22).

[166] Ryan & Toner, *supra* note 161.

[167] Under the GDPR, the European Data Protection Board is the working group constituted by representatives of each of the national data protection authorities of all the EU member states.

[168] European Data Protection Board, *Individual replies from the data protection supervisory authorities*, 2020. https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en.

complaints, most DPAs expect budgets to remain static in the upcoming year.[169] In response to these trends, the European Parliament has called for infringement proceedings against Member States accused of breaching Article 52 of the GDPR by failing to provide a budget that fosters effective performance.[170]



[171]

Data subjects and related organizations submit complaints, and data processors and controllers submit data breach notifications, to the Data Protection Authorities through online forms and supplementary guided procedures. Cases with cross-border components can be received through a DPA's website or through the Internal Market Information System (IMI), which operates as a communication tool for all EU Member States. Through IMI, DPAs can cooperate with the authorities of other concerned or lead Member States by utilizing a series of pre-translated question and answer

[169] Estelle Massé, Two Years Under the EU GDPR, Access Now (2020).

[170] *Id.* at 12.

[171] European Data Protection Board, *Individual replies from the data protection supervisory authorities* (2020). Slightly different budget figures are reported in *Deloitte, Report on EU Data Protection Authorities Part 4: Resources*, 2019.

forms, while also tracking the case's development.[172] Complaints may also be lodged by the DPA itself pursuant to the investigative and supervisory powers granted by the GDPR.

The second year of GDPR implementation has seen a dramatic increase in the quantity of complaints received by Member States. Since May 25, 2018, the United Kingdom alone has received 64,667 complaints and the German authorities 66,965.[173] Each complaint requires processing by DPA employees, and if appropriate, an investigation to determine the complaint's validity. As awareness of data protection rights increases through media reports and DPA sponsored podcasts and social media accounts, several Member States have turned to helpdesk services and online live chats in an effort to respond to the influx of complaints received by overworked complaint handlers.[174] These approaches seek to offer early-stage assessments of data privacy queries by answering questions and suggesting when potential complaints should be lodged.[175]

In 2019, Ireland's Department of Information and Assessment received 48,500 contacts related to data privacy: 22,300 emails, 22,200 phone calls, and 4,000 letters through post.[176] Ireland relies on the early-stage assessment tool as their DPA reportedly receives 150 new complaints every week – with a growing number of data subjects finding "novel ways" to apply the GDPR, according to Data Protection Commissioner Helen Dixon.[177]

[172] EUROPEAN COMM'N, SINGLE MARKET SCOREBOARD 2019 (European Comm'n 2019).

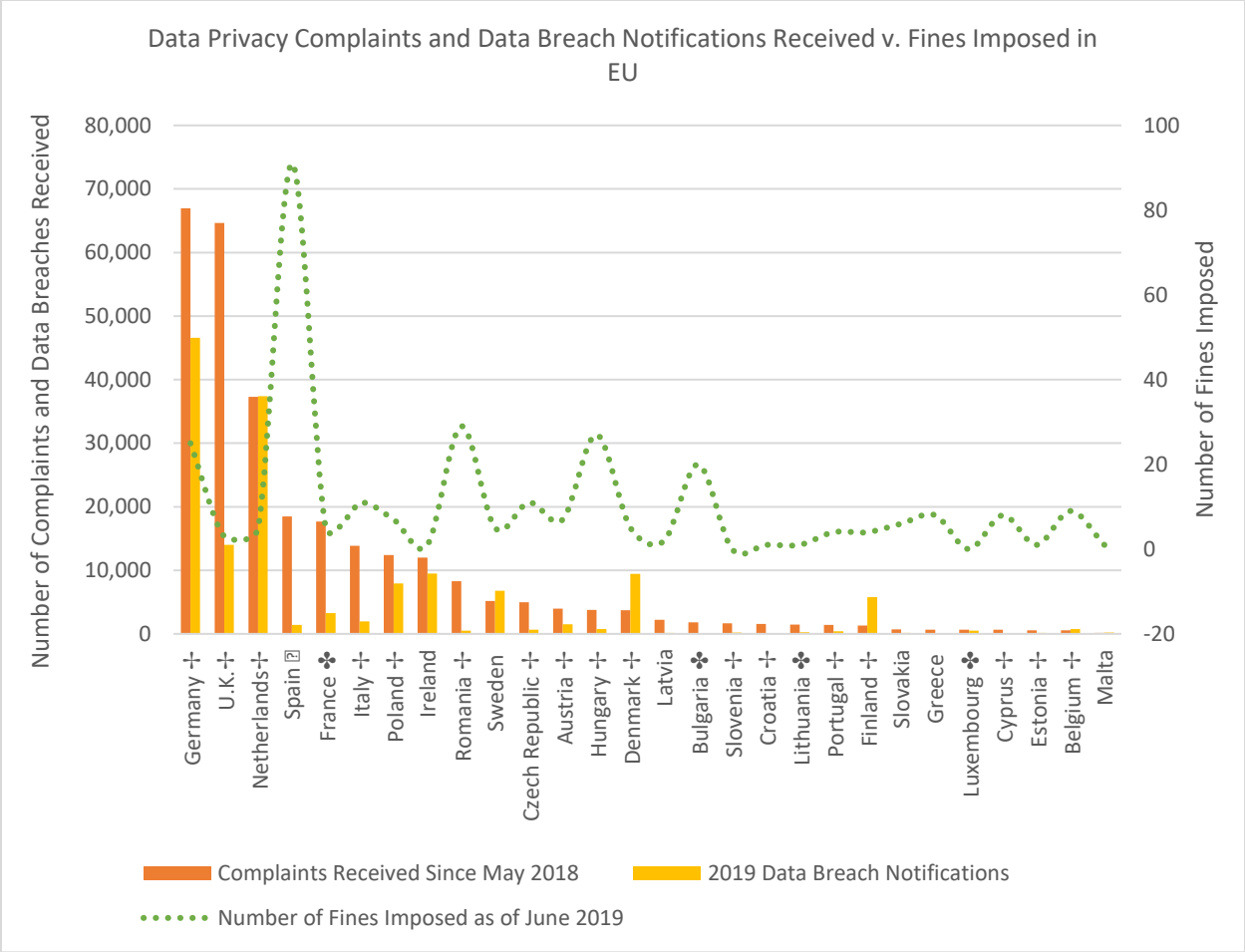
[173] *Id.*, *Individual replies from the data protection supervisory authorities* (2020).

[174] Info. Commissioner's Office, GDPR: One Year On (Info. Commissioner's Office 2019).

[175] The Commissioner for Data Protection, Annual Report (Data Prot. Comm'n 2020).

[176] *Id.* at 17.

[177] Simon Carswell, *Big Tech 'procedural Queries' Delay Decision on First Data Fines – Watchdog,* 2020 THE IRISH TIMES, Feb. 20, 2020 at (2020), https://www.irishtimes.com/business/technology/big-tech-procedural-queries-delay-decision-on-first-data-fines-watchdog-1.4178751.



178

✤ *data concluded on October 31, 2019,* ✢ *data concluded on November 30, 2019,* ≒ *data concluded on December 31, 2019.*

Despite the large volume of complaints submitted, the number of fines issued in the first two years of the GDPR's operation has remained low. By February 13, 2021, EU nations (including the UK) had issued 514 fines under the GDPR, totaling € 275,860,338.[179] Spain takes the quantitative lead, having imposed 91 fines to date since the GDPR's inception, though the Spanish DPA received 18,480 complaints and 1,434 reports of data breaches since May 25, 2018.[180] The United Kingdom and Germany — while having the largest DPAs in terms of both budget and staff compared to other Member States — have imposed just 4 and 28 fines, respectively, at the time of this writing.[181]

[178] European Data Protection Board, *Individual replies from the data protection supervisory authorities* (2020); CMS Law, *GDPR Enforcement Tracker* (2020), https://www.enforcementtracker.com.

[179] CMS Law, *GDPR Enforcement Tracker*, 2021, https://www.enforcementtracker.com/?insights.

[180] CMS Law, *GDPR Enforcement Tracker*, 2021, https://www.enforcementtracker.com

[181] *Id.*

Numerous supervisory authorities have attributed the disparity between the number of complaints received and fines issued to a lack of resources.[182]

Supervisory authorities have reported that the cooperation mechanism in which cross-border cases are compelled to operate creates significantly longer investigations and decision-making proceedings. Compulsory measures such as the exchange of relevant information and case development notifications often proceed at a slow pace.[183] Although IMI provides pre-translated forms for early stages of the complaint process, the system cannot translate documents and other correspondence relevant to the investigation and decision-making proceedings, sometimes requiring expenditures on independent translation services. The supervisory authorities of Bulgaria and Germany have noted that these translations have a considerable effect on the duration and cost of investigations, especially when cases require multiple liaises across Europe.[184]

The novel and complex legal issues presented during GDPR investigations and proceedings require substantial expenditures on legal counsel. When overseeing cross-border cases, the DPA must take into account the national procedural rules of the Member States of which an affected data subject is a citizen.[185] Italy's DPA reported that the additional legal research and dialogue required between Member States during cross-border proceedings has caused lengthened proceedings and delayed sanctions.[186] Germany, with a reported budget of €76,599,800 (more than double that of Italy's), has voiced similar complaints as their DPAs face a backlog totaling 1,200 cases, some extending as far back as 2017.[187]

Individual cases can prove extremely costly for regulators. A single investigation into Cambridge Analytica carried out by the UK data protection authority cost 2.4 million pounds (about $3.1 million) and took more than three years.[188] The investigation required it to review 42 laptops and computers, 700 TB of data, 31 servers, over 300,000 documents; and a wide range of material in paper form and from cloud storage devices.[189] After the Austrian activist Max Schrems successfully obtained a Court of Justice of the European Union decision[190] concerning cross-border data transfers to the United States, Ireland was ordered to pay his legal costs – a bill estimated to exceed €2 million euros.[191]

On average, each of the eleven lawyers in the Austrian data protection authority manages over 100 cases, cross-border and national, simultaneously.[192] With many DPA budgets failing to provide the legal resources necessary to efficiently resolve cross-border complaints, Member States like Malta have expressed the need to prioritize national complaints and limit their role in matters of regional concern.[193]

---

[182] *Id., Individual replies from the data protection supervisory authorities* (2020), available at https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en.

[183] *Id.*

[184] *Id.*

[185] European Data Protection Board, *Annual Report 2019* (2020).

[186] *Id. Individual replies from the data protection supervisory authorities* (2020).

[187] Hamburg, *Tatigkeitsbericht Datenschutz 2019* (2020).

[188] https://ftalphaville.ft.com/2020/10/06/1602008755000/ICO-s-final-report-into-Cambridge-Analytica-invites-regulatory-questions/

[189] https://techcrunch.com/2020/10/06/cambridge-analytica-sought-to-use-facebook-data-to-predict-partisanship-for-voter-targeting-uk-investigation-confirms/.

[190] Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (adopted on 23 July 2020).

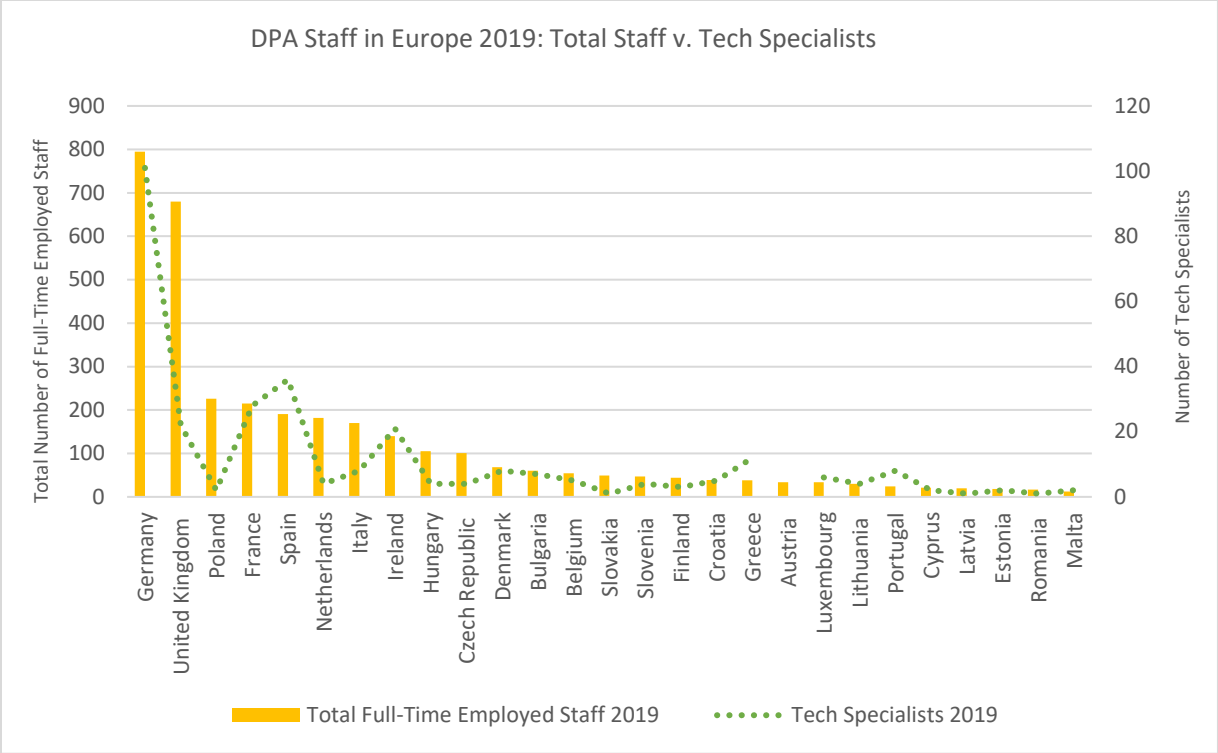
[191] Cianan Brennan, Data Protection Commission hit with massive legal bill after Facebook privacy case., Irish Examiner, Oct. 30, 2020, https://www.irishexaminer.com/news/arid-40073378.html.

[192] Austrian Supervisory Authority, *Evaluation of the GDPR under Article 97 – Questions to Data Protection Authorities/European Data Protection Supervisory Board* 6 (2020), available at https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en.

[193] *Id.*

Procedural queries by the legal teams of investigated data controllers further delay the decision-making process.[194] The DPAs oversee the regulation of data processors with revenues that are orders of magnitude larger than their budget. A notable example is Luxembourg, which allocates €5 million for data protection enforcement, including enforcing data protection against companies such as Amazon.[195]

The GDPR also creates a private right of action for material or non-material damage suffered from a breach of data privacy laws. Pursuant to Article 78, a data subject may seek a judicial remedy before the courts of the supervisory authority's Member State. A data subject can also file suit against competent supervisory authorities that (1) fail to conduct an investigation where a valid complaint exists or (2) fail to notify data subjects of developments related to the case within three months of processing.[196] Data subjects may seek recourse independently or through representation via an organization, so long as that organization's statutory objectives are aligned with the public interest and demonstrate an active presence in data rights.[197] Although at present, no data subjects or organizations have invoked Article 78 against a supervisory authority, the pressure additional legal proceedings would place on an already strained legal staff with a small budget is a matter of growing concern.[198]



[199]

According to one report, only six DPAs have more than ten technology specialists on staff contributing to investigations, while half of Europe's DPAs employ five or fewer technology

[194] Massé, *supra* note 165.

[195] *Id.* at 11.

[196] Council Directive 2016/679, art. 77, 78(2), 2016 O.J. (L 119) 1, 2.

[197] *Id.* art. 80(1).

[198] Ryan & Toner, *supra* note 158.

[199] *Id.* (vacancies included in count and full-time equivalents are rounded; data on Austria's tech specialists unavailable).

specialists.[200] Supervisory authorities like Belgium and the Czech Republic have reported that a shortage in tech investigators has limited their investigative abilities, making the collection and conservation of digital proof related to GDPR violations difficult.[201] Germany, although accounting for 29% of Europe's technology specialists, has received similar complaints from state-level DPAs.[202] The recruitment and retainment of tech specialists has also proven challenging as DPAs with restrictive budgets, 14 of which have annual budgets under €5 million, are unable to attract qualified technology experts due to uncompetitive wages.[203]

The United Kingdom's ICO has undertaken efforts to mitigate the risk of uncompetitive pay by reviewing pay arrangements against the private sector and establishing apprenticeships to attract budding specialists.[204] DPAs like Bulgaria, which lack the opportunity to undertake such reviews and programs due to limited budgets, have reported a decrease in staff as qualified employees abandon their roles due to wage dissatisfaction.[205]

B. Enforcement in the US

The United States does not have a single data privacy authority. Rather, various federal privacy laws are enforced by different agencies. In the health sector, the HIPAA is enforced principally by the Office for Civil Rights (OCR) of the DHHS. In the financial sector, the GLBA is enforced by a number of banking regulators as well as the FTC. Each of these regulators is funded separately by the US federal government. The FTC serves also as a sort of de facto privacy regulator under the rubric of regulating unfair and deceptive practices.

The following sections provide an overview of the U.S. data protection regulations at federal and state levels. They focus on the enforcement of two major privacy laws – the HIPAA and GLBA. Then, we turn to examine the cost of enforcement by the regulatory agencies.

1. HIPAA Enforcement Costs

The Office for Civil Rights (OCR) of the DHHS enforces the HIPAA Privacy, Security, and Breach Notification Rules.[206] The Office for Civil Rights also promotes broad awareness of HIPAA rights and protections.[207] It issues regulations and guidance, exacts civil monetary penalties, and pursues investigations and settlement agreements.[208] OCR funds its HIPAA enforcement efforts through both the civil monetary settlement funds it collects, as well as discretionary budget allocations.[209]

---

[200] *Id.*

[201] *Id.*, *Individual replies from the data protection supervisory authorities* (2020).

[202] *Id.*

[203] Ryan & Toner, *supra* note 158.

[204] Information Commissioner's Office, *GDPR: One year on* (2019).

[205] *Id., Individual replies from the data protection supervisory authorities* (2020).

[206] U.S. Dep't of Health & Human Services, The President's Fiscal Year 2020 Budget 147, 147-48 (2020).

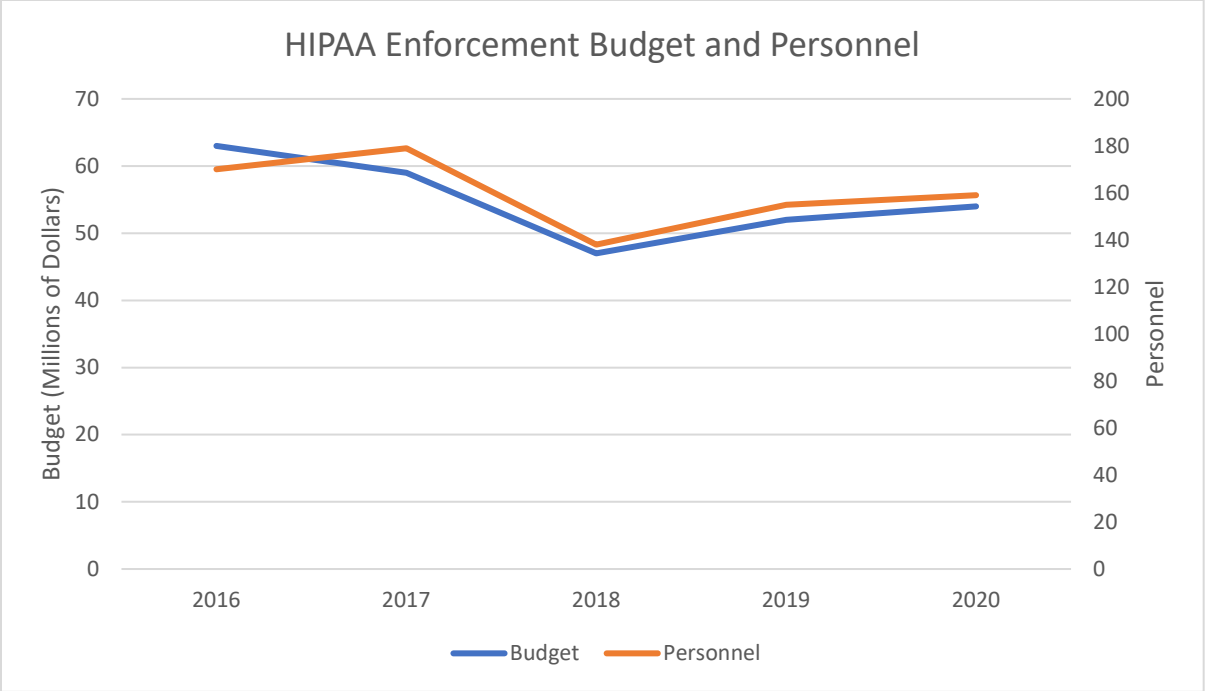
[207] *Id.*

[208] *Id.*

[209] U.S. Dep't of Health & Human Services, The President's Fiscal Year 2018 Budget 95, 95-96 (2018).

HIPAA Enforcement Budget and Personnel (Dollars in Millions)[210]					
Fiscal Year	2016	2017	2018	2019	2020
Discretionary Budget Authority	39	39	39	39	30
Civil Monetary Settlement Funds	24	20	8	13	23
Total	**63**	**59**	**47**	**52**	**53**
Number of Employees (Full-Time Equivalents)	170	179	138	155	159

[210] U.S. Dep't of Health & Human Services, The President's Fiscal Year 2020 Budget 147, 147-48 (2020); U.S. Dep't of Health & Human Services, The President's Fiscal Year 2019 Budget 125 (2020); U.S. Dep't of Health & Human Services, The President's Fiscal Year 2019 Budget 2018 Budget 95, 95-96 (2018).



From 2016 to 2019, the OCR's use of the Discretionary Budget remained consistent at $39 million but decreased to $30 million in 2020. The shortfall was more than made up by increased amounts available for enforcement from the Civil Monetary Settlement Fund, which were $8 million, $13 million, and $23 million in 2017, 2018, and 2019, respectively. The number of employees, however, has decreased in recent years.

2. FTC and Privacy and Data Security Enforcement

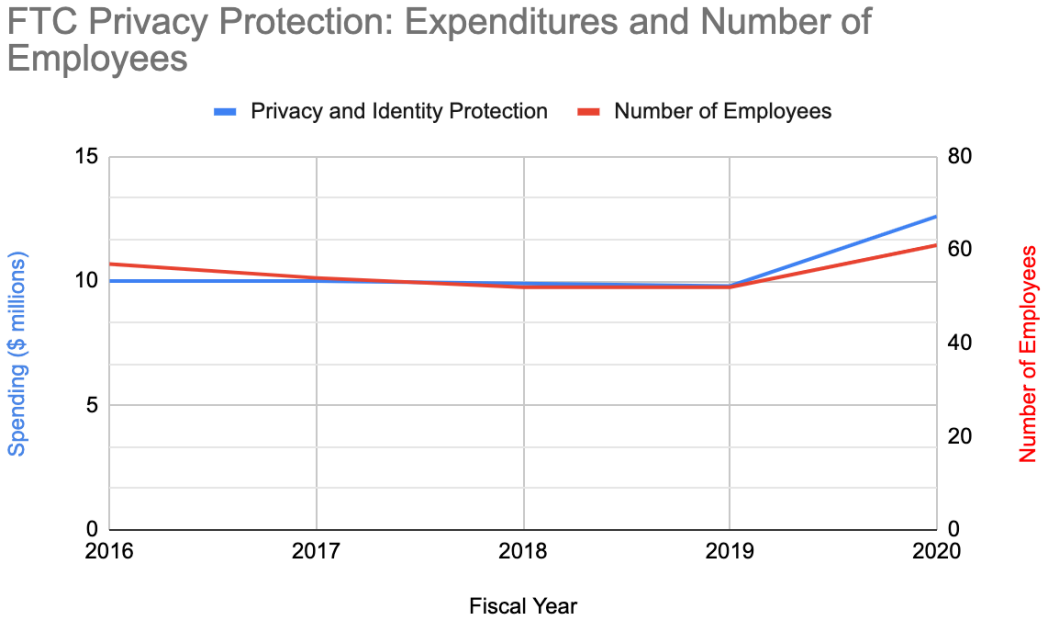
In addition to the broad power it holds under the Federal Trade Commission Act, the FTC also enforces a variety of other statutes, including the Gramm-Leach-Bliley Act, the Truth in Lending Act, the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act.[211] The FTC's enforcement thus addresses a wide range of privacy issues across a variety of industries, including social media, advertising technology, the mobile app ecosystem, and even the internet of things.[212]

While the FTC's overall enacted budget in fiscal year 2019 was $309.7 million, with 1,140 full-time employees, its budget and staff for privacy enforcement represents a small share of these larger totals. Despite an increase in workload, the FTC's budget for privacy enforcement has remained remarkably stagnant, until 2020, a year in which it also undertook a record number of enforcement actions. The FTC's privacy enforcement budget for 2021 has also been raised to a total of $13 million.[213]

[211] Fed. Trade Comm'n, *Privacy & Data Security Update* 1, 1-2 (2019).
[212] *Id.* at 2.
[213] U.S. Fed. Trade Comm'n, Fiscal Year 2021 Congressional Budget Justification 121 (2020).

FTC Spending and Workforce Dedicated to Privacy Enforcement (Dollars in Millions)[214]

Fiscal Year	2016	2017	2018	2019	2020
Privacy and Identity Protection	10	10	9.9	9.8	12.6
Number of Employees (Full-Time Equivalents)	57	54	52	52	61



3. California Consumer Privacy Act

The California Department of Justice enforces privacy laws through both its Consumer Law Unit and Privacy Unit.[215] Even prior to the passage of the California Consumer Privacy Act (CCPA), California had enforced various data protection laws including the Data Breach Notification Statute.[216]

---

[214] U.S. Fed. Trade Comm'n, Fiscal Year 2017 Congressional Budget Justification 131 (2016); U.S. Fed. Trade Comm'n, Fiscal year 2018 Congressional Budget Justification 141 (2017); U.S. Fed. Trade Comm'n, Congressional Budget Justification 121 (2020).

[215] Privacy and Data Security Law Blog (July 26, 2012), https://www.winston.com/en/privacy-law-corner/california-attorney-general-creates-privacy-enforcement-and-protection-unit.html.

[216] CAL. CIV. CODE §§ 1798.25 – 1798.78 (West 1977) (requiring a business a business or a government agency that owns or licenses unencrypted computerized data that includes personal information, as defined, to

With the coming of the CCPA, The California Department of Justice has requested an additional 23 full-time employees at an estimated cost of approximately $4.5 million per year.[217]

C. Enforcement in China

Multiple agencies are charged with enforcing Chinese privacy and cybersecurity law. While China does not have any single "supervisory authority dedicated to the protection of personal information,"[218] the Cyberspace Administration of China is generally considered the primary data protection authority in China.[219] The Ministry of Industry and Information Technology ("MIIT"), the Ministry of Public Security ("MPS") and the State Administration for Market Regulation ("SAMR") also have significant regulatory and enforcement roles with respect to data protection. Enforcement can also occur at the provincial level. In addition, sectoral regulators, such as the People's Bank of China or the China Banking and Insurance Regulatory Commission, "may also monitor and enforce data protection issues of regulated institutions within their sector."[220]

The Chinese government has in recent years launched campaigns against the misuse of information by mobile apps.[221] While the Cyberspace Administration of China's campaign focused more on shutting down apps, websites and accounts that circulated pornography and "malicious programs," MIIT, MPS and SAMR worked to address the infringement of users' rights and the illicit collecting of personal information. The following table outlines the work of their campaigns.[222]

Ministry of Industry and Information Technology (# of apps/websites)	**Ministry of Public Security (# of apps/websites)**	**State Administration for Market Regulation (# of apps/websites)**
Requested over 100 companies to rectify their policies on the collection and use of personal data.	Requested 27 companies to rectify. Issued warnings against 63 companies. Fined 10 companies. Commenced criminal investigations on 2 companies.	Investigated 1,474 cases of consumer information infringement. Fined more than 19.64 million yuan.

While there is no overall estimate of China's public sector costs in enforcing the Cybersecurity Law and its regulations, many major cities and prefectures within China have established their own branch of the Cyberspace Administration of China. The remit of these offices extends beyond data privacy. The following table illustrates the expenditures of a few of these offices for the 2020 fiscal year.

notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person).

[217] *Id.*

[218] Pernot-Leplay, *supra* note 3, at 86.

[219] DLA Piper, *supra* note 46, at 3 (2020).

[220] DLA Piper, *supra* note 46, at 144.

[221] *Id.* at 15.

[222] *Id.* at 16-17.

City or Province	Total Budget (USD/year) (millions)	Population
Hubei Province	$5.5	58,500,000
Yunan Province	$3	48,300,000
Siping City	$0.2	594,000
Chuxiong Yi Prefecture	$0.4	2,684,000
Shanghai City	$2.7	24,280,000
Suzhou City	$1.1	10,720,000

IV. Lessons for Data Privacy in Developing Countries

As the above review demonstrates, the cost of data privacy compliance can be quite high, so high that companies avoid certain jurisdictions entirely or simply ignore the laws. The GDPR can be so difficult to comply with that more than half of the EU privacy professionals surveyed in the IAPP/EY study said that their organizations were not "fully" or even "very" compliant.[223] At the same time, the cost of not having data privacy protection can be quite high as well, and results in consumers and other counterparties avoiding beneficial transactions because of the risks that the information they share will be misused. Concerns over costs of compliance or costs of enforcement might be ameliorated if stronger data protection laws make it easier for local businesses to participate in global value chains.[224] The digital economy depends on a proper legal framework that protects privacy. Based on the studies above and our discussions with experts, we offer a few recommendations below, with the particular needs of developing countries in mind.

Ensure clear rules. Rules that make clear what companies need to do both reduce costs and increase compliance. A common complaint about both EU and Chinese data privacy law among experts we spoke with was that it can be difficult to know how to comply with the law. The GDPR's complex framework (there are 173 recitals and 99 articles, and multiple guidance documents) generally requires expensive legal counsel to navigate.[225] One interviewee noted that a hospital participating in a clinical research trial with a drug company might be classified as a processor, a joint controller, or a controller in its own right, depending on the which government is enforcing the rules. A recent case from the Court of Justice of the European Union will require companies to hire lawyers to give opinions on foreign intelligence laws of every country to which the companies are transferring information outside the European Union, including the few states that have received a positive adequacy decision.[226] For their part, the Chinese rules may be highly detailed, but that detail often exists

[223] Hughes & Saverice-Rohan, *supra* note 74.

[224] The World Bank Grp., WORLD DEVELOPMENT REPORT 2020: TRADING FOR DEVELOPMENT IN THE AGE OF GLOBAL VALUE CHAINS (Caroline Freund, Aaditya Mattoo & Pol Antràs eds., World Bank Publications 2020).

[225] DataGrail, *supra* note 73, at 9 (reporting that 56% of survey respondents indicated that the GDPR regulations are complex and/or vague, and that 45% report that regulations lack a clear path to achieving compliance).

[226] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, 2020 E.C.R. I-0000.

in the form of draft rules or guidelines, rather than clearly binding law. This makes it difficult to distinguish obligations from suggestions for best practices.

Recognize the cost of data localization. Data localization is a particularly expensive and burdensome mandate. Businesses increasingly depend on cloud service providers rather than hosting their own servers or managing their own cybersecurity. Data localization imposes additional costs on local MSMEs, by requiring them to utilize local cloud services that are often more expensive than ones available globally. It can also harm domestic consumers and businesses by reducing the availability of foreign services, if those services decide that they do not wish to undertake either the expense or the additional security risks of building or renting a local data infrastructure. If the goal is to promote privacy and security, governments should insist on both as the data travels abroad.

Strive for interoperability. Multiple sets of laws greatly magnify both the complexity and expense of privacy regulation. A company that complies with the GDPR must still hire lawyers to comply with the local privacy laws of all the jurisdictions in which it operates, despite having extensive privacy protections in place already. Requiring a company operating in multiple jurisdictions to follow similar, but yet different laws, raises compliance costs with little if any practical increase in privacy protections. However, laws can be written to recognize compliance with foreign laws as one method of complying with local law, thereby allowing companies to reduce such costs and burdens. For example, a national privacy law could declare that a company that complies with the GDPR, the EU-US Privacy Shield, or the CCPA is automatically in compliance with that national privacy law. This would help draw global companies to offer services in that jurisdiction.

Consider burdens on small enterprises. Regulatory complexity poses a special challenge for micro, small, and medium-sized enterprises that do not have the resources to hire lawyers to create tailored privacy programs. It may be difficult for those working in the informal sector, for example, to comply with formal requirements such as notice. (Even an informal laborer may keep on his or her phone personal information about others, whether a friend or a business counterparty.) One response to this problem is to provide exceptions for smaller enterprises from certain requirements. For example, the California Consumer Privacy Act only covers businesses that have $25 million or more in annual revenue or that traffic in the personal information of at least 50,000 Californians. One approach is to use ex post facto liability to discipline abuses of data.

Establish a model that is conducive to cross-border data transfers. Many countries have modeled their laws on the GDPR, often in the hope of obtaining a favorable adequacy decision from the European Commission. This is understandable because any such adequacy decision would enhance opportunities to receive personal information about EU residents, making it easier to supply services to the large EU market. However, in the quarter-century following the European Data Protection Directive, only two developing countries, Argentina (in 2003) and Uruguay (in 2012), have received a favorable adequacy decision from the European Union.[227] Furthermore, the standard for receiving a favorable adequacy decision only appears to have become stricter over time. Japan was recently recognized with an

[227] Robert Carolina, *Why the EU Has Issued Relatively Few Data Protection Adequacy Determinations? A Reply*, LAWFARE (Jan. 13, 2017), (observing that Uruguay sought the status because it hoped to "attract business from Europe … that includes a large personal data processing component such as call centers, financial services, and telemedicine."). https://www.lawfareblog.com/why-eu-has-issued-relatively-few-data-protection-adequacy-determinations-reply (observing that Uruguay sought the status because it hoped to "attract business from Europe … that includes a large personal data processing component such as call centers, financial services, and telemedicine.").

adequacy decision, but only after "80 rounds of negotiations played out over 300 hours" taking place between April 2016 and January 2019.[228] Only one country is currently being considered for an adequacy decision—the Republic of Korea.[229] An adequacy decision is not the exclusive means to transfer personal data outside the European Union. The GDPR permits a variety of mechanisms for cross-border transfer of personal data, from Standard Contractual Clauses and Binding Corporate Rules to newer possibilities for certifications and codes of conduct.[230] These mechanisms are likely to prove more realistic possibilities for developing countries than the hope for a favorable adequacy decision.

One possible alternative model might lie in the EU-US Privacy Shield, which was carefully negotiated between the United States and the European Commission to protect the privacy of European Union residents when their information is transferred to the United States. The Privacy Shield represents a kind of streamlined GDPR. Companies that certified that they would comply with the extensive set of rules set forth in the Privacy Shield were allowed to receive that data. Some 5,300 companies signed up, certifying compliance. On July 16, 2020, the Court of Justice of the European Union struck down the EU-US Privacy Shield on the ground that it did not provide sufficient legal rights to European residents to challenge U.S. foreign surveillance.[231] If that issue can be resolved (through, for example, extending legal rights to challenge surveillance to foreigners), the Privacy Shield might serve as a useful model for other nations to permit interoperability. Experts we spoke with affirmed that companies took compliance with the Privacy Shield seriously. While the Privacy Shield was designed to facilitate cross-border transfer of data from the European Union to the United States,[232] it represents a workable attempt to meet core European Union concerns with data privacy in a way that companies seem to manage. Its principles thus could well serve as a model for national privacy laws themselves. Companies seeking to comply with the Privacy Shield must (1) publish a privacy policy with certain specified information; (2) provide option to opt-out (opt-in for sensitive data) for disclosures to third parties or for uses for a materially different purpose than that for which the data was provided; (3) enter into contracts to protect data when sharing data with third parties or agents; (4) take reasonable and appropriate measures to protect security of data; (5) limit processing to authorized purposes; (6) provide rights to access, correct, amend, or delete; and (7) provide recourse for complaints.[233] In addition, companies must abide by 16 supplementary principles.

***

Getting data privacy law right is critical for every country in the twenty-first century. Our study shows that even the United States and the EU do not expend sums far outside the reach of many developing nations to enforce data privacy law. Indeed, the smallest European nations spend only half-a-million dollars annually for their data privacy authority. Furthermore, while costs of compliance for private businesses vary significantly, developing states could take steps such as relaxed mandates for small and medium-sized businesses, or ex post facto liability rules for negligent or intentional abuses

---

[228] Martin Braun, Frederic Louis, Itsiq Benizri, *The European Commission Adopts Adequacy Decision On Japan,* WilmerHale (Jan 24, 2019), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20190124-the-european-commission-adopts-adequacy-decision-on-japan.

[229] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[230] See GDPR, arts 44-49. Indeed, our survey respondents indicated that they rely principally on standard contractual clauses for cross-border data transfer from the EU. Privacy Survey, at 23.

[231] *See* Chander, *supra* note 52.

[232] Aaditya Mattoo & Joshua P. Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution*, 21 23 J. INT'L EC. L. 769, 771 (2018) ("the EU–US Privacy Shield offers a way of resolving the conflict between regulatory heterogeneity and international data flows").

[233] Privacy Shield Framework, *Privacy Shield Overview*, https://www.privacyshield.gov/program-overview.

of personal data. Developing states might also engage regionally and bilaterally with other jurisdictions to effectively distribute the costs of enforcement through systems of mutual recognition.

As the above review demonstrates, the cost of data privacy compliance can be quite high, so high that companies avoid certain jurisdictions entirely or simply ignore the laws. The GDPR can be so difficult to comply with that more than half of the EU privacy professionals surveyed in the IAPP/EY study said that their organizations were not "fully" or even "very" compliant.[234] At the same time, the cost of not having data privacy protection can be quite high as well, and results in consumers and other counterparties avoiding beneficial transactions because of the risks that the information they share will be misused. Concerns over costs of compliance or costs of enforcement might be ameliorated if stronger data protection laws make it easier for local businesses to participate in global value chains.[235] The digital economy depends on a proper legal framework that protects privacy.

The study also reveals the need for further inquiry. Private companies are reluctant to publish information about the costs of compliance, which might be perceived as either too little (by consumers) or too much (by shareholders). Might particular data privacy obligations such as the right to data access, to redress, to reasonable cybersecurity, for example, offer particularly cost-effective privacy? Governments should review their own enforcement efforts, including whether the resources they deploy are sufficient to regulate the growing digital economy. How effective are different types of government enforcement efforts (such as audits, sanctions, or guidance regarding best practices)? Governments could gather more data from companies on their compliance expenditures.

Understanding costs is a critical step towards achieving privacy.

[234] Hughes & Saverice-Rohan, *supra* note 74.

[235] The World Bank Grp., WORLD DEVELOPMENT REPORT 2020: TRADING FOR DEVELOPMENT IN THE AGE OF GLOBAL VALUE CHAINS (Caroline Freund, Aaditya Mattoo & Pol Antràs eds., World Bank Publications 2020).