SMU | Dedman School of Law

SMU Law Review

Volume 74 | Issue 4 Article 6

2021

Achieving Privacy

Anupam Chander
Georgetown University Law Center

Author(s) ORCID Identifier:
Anupam Chander: https://orcid.org/0000-0002-8820-4870

Meaza Abraham
Georgetown University Law Center

Author(s) ORCID Identifier:
Anupam Chander: https://orcid.org/0000-0002-8820-4870

Sandeep Chandy
Georgetown University Law Center

Author(s) ORCID Identifier:
Anupam Chander: https://orcid.org/0000-0002-8820-4870

Yuan Fang
Georgetown University Law Center

Author(s) ORCID Identifier:
Anupam Chander: https://orcid.org/0000-0002-8820-4870

Dayoung Park
Georgetown University Law Center

Author(s) ORCID Identifier:
Anupam Chander: https://orcid.org/0000-0002-8820-4870

See next page for additional authors

Recommended Citation

Anupam Chander et al., *Achieving Privacy*, 74 SMU L. Rev. 607 (2021)
https://scholar.smu.edu/smulr/vol74/iss4/6

Achieving Privacy

Authors

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

Author(s) ORCID Identifier:

Anupam Chander: https://orcid.org/0000-0002-8820-4870

ACHIEVING PRIVACY

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

Is privacy a luxury for the rich? 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 the costs of compliance and to summarize national budgets for enforcement. Our study suggests that, while privacy may indeed prove costly for companies to implement and may present a special burden for small and medium-sized businesses, it is not too costly for governments to enforce. Indeed, the European Union, seen as a global champion of privacy, expends less than a dollar a year per citizen on data protection enforcement. Effective data protection agencies are not prohibitively costly, even for small administrations, especially if they collaborate through regional bodies. This study will help inform governments as they fashion and implement privacy laws to address the "privacy enforcement gap"—the disparity between privacy on the books and privacy on the ground.

TABLE OF CONTENTS

* Professor of Law, Georgetown University. This study was commissioned by the World Bank in connection with its 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. We are especially grateful to Martín Molinuevo, Michael Joseph Ferrantino, Vivien Foster, and Daria Taglioni, all of the World Bank, and to commentators at the World Development Report seminar on Data and Trade for very helpful comments. We also thank Hannah Luke, Kathrine Maldonado, Benjamin Rice, and their SMU Law Review colleagues for excellent editing. All the views, and any errors, expressed herein are our own.

** 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.

I. INTRODUCTION

IS privacy a luxury for the rich?[1] This Article seeks to understand how much data privacy laws cost to implement and enforce. Relying on industry surveys, government studies, and government agency budgets, this Article compares the costs of private sector implementation and public sector enforcement for the United States, the 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 attention to 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

1. Julia Angwin, Opinion, *Has Privacy Become a Luxury Good?*, N.Y. TIMES (Mar. 4, 2014), https://www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html [https://perma.cc/9AJ4-XVDL].

ground."[2] A decade ago, Kenneth Bamberger and Deirdre Mulligan observed that "no one has conducted a sustained inquiry into how corporations actually manage privacy and what motivates them."[3] Their study described how companies were responding to regulations and enforcement.[4] But even a decade later, we know too little about the costs of compliance or enforcement. Despite the rapid embrace of laws designed to regulate the use of personally identifiable information, there is a remarkable scarcity of studies about their costs.[5] 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 of compliance with new regulations for small and medium-sized companies. Governments too may also be concerned about the additional costs of enforcing 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.[6] 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.[7] Benefits of data privacy are difficult to quantify outside of clear invasions like identity theft.[8] Not only does data privacy have enormous benefits for

2. Filippo Lancieri, *Narrowing Data Protection's Enforcement Gap*, 74 ME. L. REV. (forthcoming 2022) (manuscript at 1) (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. *Id.* at 251.

5. We discuss the existing studies in Part III 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.

6. *See, e.g.*, 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) ("[F]reedom from surveillance. . . 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).

7. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12, (Dec. 10, 1948); International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171 (registered ex officio Mar. 23, 1976); Charter of Fundamental Rights of the European Union 326/02, arts. 7, 8, 2012 O.J. (C 326) 397.

8. While certain harms caused by data abuse are more readily calculable—such as those from identity theft—the harms 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 Health Insurance Portability and Accountability Act (HIPAA) rules in 2013, the Department of Health and Human Services (DHHS) noted that it was "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).

individuals, but it also helps companies build and maintain the trust of their users and their business partners.[9] Indeed, understanding the costs of compliance and enforcement will better enable developing countries to design their laws and enforcement structures.

Across the world, nations are establishing data privacy rules.[10] The datafication of the economy means that few companies or individuals are untouched.[11] Laws regulating the use of personally identifiable data are a necessary foundation of the digital economy.[12] Companies are collecting data at an unprecedented rate as computers mediate more and more of our lives.[13] Laws help prevent abuse and thus help build trust as individuals interact in an increasingly digitized world.[14] Data privacy is a necessity not just in richer nations, but in poorer ones as well.[15]

Achieving data privacy presents special challenges in the developing world—both for companies and governments.[16] Micro, small, and medium-sized companies may lack the resources to ensure compliance with complicated laws.[17] If compliance is too expensive, businesses may simply ignore the law or avoid the jurisdiction altogether. Governments, their resources already stretched, may not be able to devote sufficient resources to privacy enforcement.[18]

Data privacy is also increasingly critical to international trade.[19] As data travels across the world, governments and individuals seek to ensure that privacy protections travel alongside the data.[20] At the same time, data regulations that mandate data localization impose special costs; for example, data regulations can be used to disfavor foreign service

9. Michael Fimin, *Five Benefits GDPR Compliance Will Bring to Your Business*, FORBES (Mar. 29, 2018, 7:30 AM), https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/?sh=7af021b4482f [https://perma.cc/LB6A-94AE].

10. *Data Protection and Privacy Legislation Worldwide*, U.N. CONF. ON TRADE & DEV., https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx [https://perma.cc/EVJ8-W2AR].

11. Irving Wladawsky-Berger, *How Datafication Will Redefine Business and Society*, WALL ST. J. (June 12, 2015, 12:29 PM), https://www.wsj.com/articles/BL-CIOB-7334 [https://perma.cc/T9MA-D2TS].

12. Ralph Schroeder, *Big Data Business Models: Challenges and Opportunities*, 2 COGENT SOC. SCIS. 1, 12–13 (2016).

13. Wladawsky-Berger, *supra* note 11.

14. *See Protecting Consumer Privacy and Security*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security [https://perma.cc/6AQN-TAV2].

15. *See* Linnet Taylor & Dennis Broeders, *In the Name of Development: Power, Profit, and the Datafication of the Global South*, 64 GEOFORUM 229, 236 (2015).

16. U.N. Conference on Trade and Development, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, at xii, U.N. Doc. UNCTAD/DTL/STICT/2016/1 (2016).

17. *Id.*

18. *Id.*

19. WORLD BANK GRP., WORLD DEVELOPMENT REPORT 2021: DATA FOR BETTER LIVES 237 (2021) [https://perma.cc/8UUQ-CRE7].

20. *Id.* at 238.

providers.[21]

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.[22] This 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 are already in place, we can illuminate the experience of companies complying with those laws. We also describe the costs of enforcement.

This Article proceeds as follows. Part II begins by briefly characterizing three of the major data protection regimes: the European Union, the United States, and China. Part III then describes the costs of private sector compliance with respect to each of these three regimes. Part IV turns to the costs of public enforcement, again for these three different jurisdictions.

II. THREE APPROACHES TO DATA PRIVACY: THE E.U., THE UNITED STATES, 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 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 E.U. 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 the processing of personal data is necessary for the performance of a contract.[23] If that basis is consent, that consent must be "freely given, specific, informed and unambiguous."[24] Personal data must be processed lawfully, fairly,

21. Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677, 679 (2015); Martina Francesca Ferracane & Erik van der Marel, Regulating Personal Data: Data Models and Digital Services Trade 3 (2021), https://openknowledge.worldbank.org/bitstream/handle/10986/35308/Regulating-Personal-Data-Data-Models-and-Digital-Services-Trade.pdf?sequence=1&isAllowed=Y [https://perma.cc/ZH25-6WC4].

22. Rachel F. Fefer & Kristin Archick, Cong. Rsch. Serv., IF10896, EU Data Protection Rules and U.S. Implications 2 (2020); Alexa Lee, *Personal Data, Global Effects: China's Draft Privacy Law in the International Context*, New Am. (Jan. 4, 2021), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/personal-data-global-effects-chinas-draft-privacy-law-in-the-international-context [https://perma.cc/KC6E-NR42].

23. Commission Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 6, 2016 O.J. (L 119) 1, 36 [hereinafter GDPR].

24. *Id.* art. 4(11).

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."[25] 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.[26] The GDPR mandates that data controllers and processors adopt the principle of "privacy by design," seeking to implement data-protection principles in their products and taking into account costs of implementation and risks for data subjects.[27] For data processing activities that pose high risks to data subjects, the GDPR requires that data controllers carry out data protection impact assessments.[28] 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.[29] The GDPR even goes beyond data privacy by, for example, giving each person the right to choose to not be subject to automated decision-making that produces legal effects on that person.[30]

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.[31] A risk-based approach allows for the differential application of the GDPR according to the type of data, the nature and size of the organization, and the uses of that data.[32] 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.[33] Examples may include processing based on new technologies and extensive automated decision-making with legal effects.[34] The procedures required for such high risk data collection and processing may include, for example, mandatory data protection impact assessments in which processing risks are identified, safeguards are presented, and (in certain cases) consultation with a Data Protection Authority is required before proceeding.[35] Furthermore, organizations are required to take the appropriate technical and organiza-

25. *Id.* art. 5.
26. *Id.* arts. 13–21.
27. *Id.* art. 25.
28. *Id.* art. 35.
29. *Id.* art. 37.
30. *Id.* art. 22.
31. *See* European Commission, *The GDPR: New Opportunities, New Obligations*, at 3 (2018), https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-sme-obligations_en.pdf [https://perma.cc/SYB7-6RM4].
32. GDPR News, *What Is High Risk Under GDPR?*, COMPLIANCE JUNCTION (Dec. 22, 2017), https://www.compliancejunction.com/high-high-risk-gdpr [https://perma.cc/69PS-9YR8].
33. *Id.*
34. *Id.*
35. *Id.*; GDPR, *supra* note 23, arts. 35–36.

tional measures to properly safeguard personal data pursuant to the regulation's policy of data protection by design and default.[36]

B. Compliance Under the U.S. Data Privacy Regime

The U.S. data privacy regime lacks a comprehensive law that regulates the collection and processing of personal data of U.S. residents by private parties.[37] While there are constraints against government information collection through both the U.S. Constitution and an extensive statutory framework regulating *government* use of personal data, there is no similarly broad federal regulatory privacy law regulating private parties.[38] 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.[39] 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.[40] Sectoral laws include the Health Insurance Portability and Accountability Act (HIPAA),[41] covering the health industry, and the Gramm–Leach–Bliley Act (GLBA),[42] covering the financial sector. In addition, the Federal Trade Commission Act (FTCA) gives the Federal Trade Commission (FTC) broad authority to regulate data practices if they constitute "unfair or deceptive acts or practices in or affecting commerce."[43] Through the FTCA, the FTC serves as the nation's de facto privacy regulator, and its settlements create a kind of common law of privacy.[44]

HIPAA imposes an extensive set of privacy protections for personal health data gathered by covered entities, including hospitals, healthcare providers, and health insurers.[45] Not only must health plans and healthcare providers give patients a written notice of their privacy practices, they must also "maintain reasonable and appropriate administrative,

36. GDPR, *supra* note 23, art. 25.

37. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, Council on Foreign Rels. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/U33F-DLN3].

38. *See* Stephen P. Mulligan & Chris D. Linebaugh, Cong. Rsch. Serv., IF11207, Data Protection and Privacy law: An Introduction 1 (2019); 5 U.S.C. § 552a(b) (regulating agency disclosure of records).

39. O'Connor, *supra* note 37.

40. *See, e.g.*, *Snapchat Settles FTC Charges that Promises of Disappearing Messages Were False*, Fed. Trade Comm'n (May 8, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were [https://perma.cc/6RE8-88WT].

41. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

42. Gramm–Leach–Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

43. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240, 247–48 (3d Cir. 2015); 15 U.S.C. § 45(a).

44. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 585–86 (2014).

45. C. Stephen Redhead, Cong. Rsch. Serv., RS20500, Medical Records Privacy: Questions and Answers on the HIPAA Final Rule (2001).

physical, and technical safeguards to ensure the integrity and confidentiality of the information" and "to protect against any reasonably anticipated threats."[46] These safeguards include "designating a privacy official, training employees, and developing a system of sanctions for employees who violate the entity's policies."[47] HIPAA also requires 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 systems."[48] The DHHS has extensively used its rule-making authority to elaborate on the statute.

The GLBA (also known as the Financial Modernization Act) regulates the use of non-public personal information by institutions or businesses engaged in financial activities such as banks, insurers, and brokerage firms.[49] The GLBA empowers the FTC to enforce the obligations that establish standards for financial institutions relating to administrative, technical, and physical information safeguards.[50] 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.[51]

California's Consumer Privacy Act (CCPA), which went into effect at the beginning of 2020, will have a significant impact, especially on larger enterprises.[52] 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 half or more of their revenue from selling consumers' personal information.[53] 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.[54] The CCPA requires businesses to disclose the types and sources of personal data the business collects from customers and grants California residents the right to access and delete personal information.[55] The CCPA thus relies largely on a notice and consent model. Rights under the CCPA include the right to be notified about what personal information is col-

46. § 1173(d)(2), 110 Stat. at 2026.
47. REDHEAD, *supra* note 45, at 5.
48. § 1173(d)(1), 110 Stat. at 2025–26.
49. Gramm–Leach–Bliley Act, Pub. L. No. 106-102, § 501, 113 Stat. 1338, 1436 (1999).
50. *Id.* §§ 501, 505, 113 Stat. at 1436–1437, 1440.
51. *Id.* § 509, 113 Stat. at 1444.
52. CAL. CIV. CODE §§ 1798.100 to .199.100 (Deering 2018); *see* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1734 (2021).
53. CIV. § 1798.140. Accordingly, beyond curtailing certain forms of punishment, the Eighth Amendment now—in addition to placing restraints on prison officials—also imposes significant duties upon these officials
54. *See* Chander et al., *supra* note 52, at 1772.
55. CIV. §§ 1798.100, 1798.105.

lected and the right to opt out of the sale of that information.[56] The CCPA-based right to access information will require substantial reworking of data practices at companies that have not previously created systems to manage the personal information they store, such as data inventory mapping.[57] The opt-out feature provided by the CCPA will also require companies to create mechanisms for such requests and treat data differently depending on the choices consumers have made.[58] The CCPA is principally enforced by California's Attorney General.[59] In November 2020, California voters passed the California Privacy Rights Act, which adopts principles of data minimization and purpose limitation, requires risk audits for high-risk activities, and will establish a new California Privacy Protection Agency when it goes into full effect in 2023.[60]

C. Compliance Under the Chinese Data Privacy Regime

China's data privacy regime is the newest of the three jurisdictions described in this Article. It is best understood against the backdrop of China's development as a leading technological power that has simultaneously sought to maintain strong governmental control and public order.[61] China's approach reflects a nearly decade-old "national strategy to embrace 'big data.'"[62] 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.[63] A fourth goal, the promotion of China's technological advancement, has also been a key consideration in its implementation of data protection laws.[64]

---

56. *Id.* §§ 1798.110, 1798.120.

57. Mark Brennan, James Denvil & Aaron Lariviere, *The Challenge Ahead—Data Mapping and the CCPA*, Hogan Lovells (Sept. 19, 2018), https://www.engage.hoganlovells.com/knowledgeservices/news/the-challenge-ahead-data-mapping-and-the-ccpa_1 [https://perma.cc/9AJ3-QSTD].

58. George P. Slefo, *Bracing for Sweeping New Data Privacy Law; How Brands Are Preparing as the California Consumer Privacy Act Becomes a Reality in 2020*, AdAge (Oct. 14, 2019), https://adage.com/article/news/how-brands-are-preparing-californias-privacy-act-becomes-reality-2020/2205586 [https://perma.cc/3MEC-ZVFE].

59. *See* Civ. § 1798.155.

60. *See California Privacy Rights Act (CPRA)*, Perkins Coie, https://www.perkinscoie.com/en/practices/security-privacy-law/california-privacy-rights-act-cpra.html [https://perma.cc/PD8R-2J36].

61. *See* Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?*, 8 Penn. St. J.L. & Int'l Affs. 49, 69 (2020).

62. 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, 227 (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 Am. (May 28, 2020), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-scholar-outlines-stakes-new-personal-information-and-data-security-laws-translation [https://perma.cc/Q8ZP-U99Y].

63. Pernot-Leplay, *supra* note 61, at 69.

64. James L. Schoff & Asei Ito, *Competing with China on Technology and Innovation*, Carnegie Endowment for Int'l Peace (Oct. 10, 2019), https://carnegieendowment.org/

State security has been a focus of Chinese data policy from the start.[65] 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, but instead might be used to create "an ennobling space where netizens complete their transformation into perfect citizens."[66] Typically, data protection policies are focused on the protection of the data of individuals and not on the promotion of state interests.[67] 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.[68] 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.[69]

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.[70] 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.[71] App providers are also required to register the real names of their users, as part of an information content review.[72] The Cybersecurity Law also imposes real name registration obligations for information publishing and instant messaging services.[73] The ability to identify the user can be useful for the government in identifying lawbreakers, though human rights advocates have raised concerns about such requirements.[74]

The cornerstone of China's data protection law can be found in the Cybersecurity Law enacted in 2016 by the Standing Committee of the

---

2019/10/10/competing-with-china-on-technology-and-innovation-pub-80010 [https://perma.cc/24WM-Y7CU].

65. *See* Lorand Laskai, *Nailing Jello to a Wall*, *in* CONTROL 192, 194 (Jane Golley, Linda Jaivin & Luigi Tomba eds., 2016).

66. *Id.* at 195.

67. Pernot-Leplay, *supra* note 61, at 69.

68. Laskai, *supra* note 65, at 197.

69. Pernot-Leplay, *supra* note 61, at 104–05.

70. *China: Cyberspace Administration Releases New Rules on Mobile Apps*, LIBR. CONG. (July 26, 2016), https://www.loc.gov/item/global-legal-monitor/2016-07-26/china-cyberspace-administration-releases-new-rules-on-mobile-apps [https://perma.cc/5TX4-SC3R].

71. *Id.*

72. *Id.*

73. JONES DAY, IMPLEMENTING CHINA'S CYBERSECURITY LAW 2 (2017), https://www.jonesday.com/files/upload/Implementing%20Chinas%20Cybersecurity%20Law.pdf [https://perma.cc/4SBK-D4GS].

74. Bethany Allen-Ebrahimian, *The 'Chilling Effect' of China's New Cybersecurity Regime*, FOREIGN POL'Y (July 10, 2015, 3:27 PM), https://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security [https://perma.cc/4BTQ-GKRC].

National People's Congress.[75] That law imposes numerous data protection obligations on "network operators," which are defined broadly to include network owners, managers, and network service providers.[76] A central obligation is the requirement to obtain consent before collecting or sharing personal information.[77] 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.[78] While non-binding, the 2018 Specification has proved highly influential, establishing what has been described as a set of best practices related to data protection.[79] The government relies on this standard for enforcement actions.[80] The 2018 Specification often goes beyond the statutory text; for example, while the Cybersecurity Law requires only that companies do not gather personal information *unrelated* to the services they provide, the Specification goes further to limit collection only to information that is *necessary*.[81]

A revised Specification went into effect on October 1, 2020.[82] This 2020 Specification mandates affirmative (opt-in) consent for processing sensitive personal information.[83] It also requires fully informed consent for the

---

75. Wangluo Anquan Fa (网络安全法) [Cybersecurity Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017).

76. *Id.* arts. 9, 76.

77. *Id.* arts. 22, 41, 42.

78. *See* Pernot-Leplay, *supra* note 61, at 76 n.119; Yan Luo & Phil Bradley-Schmieg, *Inside Privacy: Updates on Developments in Data Privacy and Cybersecurity*, COVINGTON (Jan. 25, 2018), https://www.insideprivacy.com/international/china/china-issues-new-personal-information-protection-standard [https://perma.cc/2P3N-MRCW].

79. *China Releases Draft Amendments to the Personal Information Protection Standard,* COVINGTON (Feb. 11, 2019), https://www.cov.com/-/media/files/corporate/publications/2019/02/china_releases_draft_amendments_to_the_personal_information_protection_standard.pdf [https://perma.cc/6MF8-9CT6]. Our interviewees confirmed that the Specifications were taken seriously, despite not having the force of law. *See infra* note 113 and accompanying text.

80. Jenny (Jia) Sheng & Chunbin Xu, *China Publishes Best Practices for Protection of Perosnal Information*, PILLSBURY, https://www.pillsburylaw.com/en/news-and-insights/china-publishes-best-practices-for-protection-of-personal-information.html[https://perma.cc/2A4Q-CR7M].

81. Cybersecurity Law of the People's Republic of China, *supra* note 75, art. 41; Pernot-Leplay, *supra* note 61, at 94–95.

82. Michelle Chan, Clarice Yue & Tiantian Ke, *China Cybersecurity Law Update: Two New National and Industry Standards: Personal Information Specification and Personal Financial Information Specification Officially Published!*, BIRD & BIRD (Apr. 2020), https://www.twobirds.com/en/news/articles/2020/china/china-cybersecurity-law-update-two-new-national-and-industry-standards[https://perma.cc/8S6N-NQZY].

83. *Id.*; HOGAN LOVELLS, THE DUST HAS FINALLY SETTLED—THE LONG JOURNEY OF CHINA'S NEW PERSONAL INFORMATION SECURITY SPECIFICATION 1–2 (Apr. 2020). An official English translation of the 2020 Specification is available here: https://www.tc260.org.cn/front/postDetail.html?id=20200918200432 [https://perma.cc/BY9J-XZ82].

collection and use of biometric information.[84] 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.[85] The 2020 Specification establishes new rules for companies that personalize information based on profiling, including targeted advertising.[86] The 2020 Specification provides detailed rules on the obligations of both personal information controllers and the third parties with which they share information.[87] 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.[88] 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.[89]

The 2020 Specification adopts aspects of the GDPR model.[90] 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).[91] The guidance also imposes duties on data controllers with respect to third parties with whom they share information.[92]

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."[93] For example, unlike the European Union, where consent must be explicit, the Chinese interpretation of consent seems to permit implied consent, at least for non-sensitive personal information.[94] An individual's right to port their 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.[95] Yet at certain other points, the Chinese law, at least on its face, can be even more demanding than the E.U. law.[96] For example, the Cybersecurity Law

84. HOGAN LOVELLS, *supra* note 83, at 1–2, 6.

85. "*Personal Information Security Regulations" English Version Announced*, NAT'L INFO. SEC. STANDARDIZATION TECH. COMM. (Sept. 20, 2020), https://www.tc260.org.cn/front/postDetail.html?id=20200918200432 [https://perma.cc/9SEP-Z487].

86. HOGAN LOVELLS, *supra* note 83, at 2.

87. *Id.* at 5–6.

88. *Id.* at 5.

89. *Id.* at 6.

90. *Id.* at 1.

91. *Id.*

92. *Id.* at 5.

93. Pernot-Leplay, *supra* note 61, at 82.

94. *Id.* at 84–85. The proposed amendments to the Standard also make provision for implied consent. *Id.*

95. *Id.* at 101.

96. *Id.* at 103.

seems to make consent the exclusive basis for information collection, unlike the E.U. law, which allows a variety of bases for collecting personal information, including a category of "legitimate interests."[97] 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";[98] this would enhance the ability to regulate data for security-related goals.

On August 20, 2021, the Standing Committee of the National People's Congress adopted the Personal Information Protection Law of the People's Republic of China (PIPL), the first legislation focused on protecting personal data in China. The Wall Street Journal declared it "one of the world's strictest data-privacy laws," and many compared the PIPL to the GDPR.[99] The PIPL requires that personal information only be processed where there is a "clear and reasonable purpose," that the collection of personal information be minimized and not excessive, and that processors ensure the security of personal information. It also requires processors to carry out risk assessments prior to engaging in certain activities.[100] In some ways, the PIPL is stricter than the GDPR.[101] Unlike the GDPR, businesses cannot rely on "legitimate interests" to collect and process data. Furthermore, individual consent may be needed in certain circumstances when it would not be required under the GDPR.[102] In other aspects, the PIPL is less strict. For example, the PIPL provides an additional legal basis for processing when that information has already been lawfully disclosed.[103] The PIPL took effect on November 1, 2021.

Security is also a key motivation for other aspects of the data regime. In comparison to the United States' all-permissive approach to cross-border data flow and the European Union's careful control on outward flows of personal data, China has moved towards more restrictive policies to keep data within its own borders.[104] Certain important entities must store

97. *Id.* at 83–84; GDPR, *supra* note 23, art. 6.

98. KEN DAI & JET DENG, DENTONS, 2019 CHINA DATA PROTECTION & CYBERSECURITY ANNUAL REPORT 11 (2020).

99. Eva Xiao, *China Passes One of the World's Strictest Data-Privacy Laws*, WALL ST. J. (Aug. 20, 2021, 4:55 AM), https://www.wsj.com/articles/china-passes-one-of-the-worlds-strictest-data-privacy-laws-11629429138 [https://perma.cc/7G3U-TK9G].

100. *China Passes the Personal Information Protection Law, to Take Effect on November 1*, GIBSON DUNN (Sep. 10, 2021), https://www.gibsondunn.com/china-passes-the-personal-information-protection-law-to-take-effect-on-november-1 [https://perma.cc/KL2G-E7N7].

101. Catherine Zhu, *Is China's New Personal Information Privacy Law the New GDPR?*, BLOOMBERG L. (Sept. 17, 2021, 4:01 AM), https://news.bloomberglaw.com/banking-law/is-chinas-new-personal-information-privacy-law-the-new-gdpr [https://perma.cc/K8FY-XU7K].

102. *Id.*

103. LATHAM & WATKINS, CHINA INTRODUCES FIRST COMPREHENSIVE LEGISLATION ON PERSONAL INFORMATION PROTECTION 1, 3 (September 8, 2021), https://www.lw.com/thoughtLeadership/china-introduces-first-comprehensive-legislation-on-personal-information-protection#:~:text=ON%20August%2020%2C%202021%2C%20the,effect%20on%20November%201%2C%202021 [https://perma.cc/9KFK-XF6X].

104. Richard D. Taylor, *"Data Localization": The Internet in the Balance*, 44 TELECOMM. POL'Y 1, 8 (2020).

personal information in China unless they pass a Cyberspace Administration of China security assessment. Furthermore, when transferring personal information outside China, the processor must "inform the data subjects of the transfer, obtain their specific consent to the transfer, and ensure that the data recipients satisfy standards of personal information protection similar to those in the PIPL."[105]

Chinese practitioners we interviewed suggested that a key cost of compliance was in setting up privacy management systems, including data mapping. One significant challenge was to change internal corporate culture to prioritize privacy.

III. COSTS OF PRIVATE COMPLIANCE

The costs of complying with privacy law vary 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 European Union 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.[106] Another study, meanwhile, found an average 2018 budget focused on GDPR compliance of $13.2 million, rising to $13.6 million in 2019.[107] Estimates for compliance with U.S. privacy laws 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 E.U. privacy regime to be the costliest of the three frameworks. They described compliance with the U.S. regime as less expensive, whether for large or small firms, and compliance with Chinese privacy laws as the least expensive—though that may be due to a lack of awareness of the law. Among our respondents, cybersecurity costs appeared to be more significant with respect to compliance with Chinese and U.S. laws than compliance with E.U. law. The E.U. compliance costs seem to be significantly skewed towards personnel, both in-house personnel and outside consultants.

As the wide ranges of the estimates might suggest, the data is inherently limited. There is no consistent framework for analyzing the costs of

105. *China Passes the Personal Information Protection Law, to Take Effect on November 1*, *supra* note 100.

106. INT'L ASS'N PRIV. PROS., IAPP-EY ANNUAL PRIVACY GOVERNANCE REPORT 2019, at 28 (2019).

107. PONEMON INST., KEEPING PACE IN THE GDPR RACE: A GLOBAL VIEW OF GDPR PROGRESS IN THE UNITED STATES, EUROPE, CHINA, AND JAPAN 27 (2019), [hereinafter PONEMON INST., KEEPING PACE] https://mcdermott-will-emery-2793.docs.contently.com/v/keeping-pace-in-the-gdpr-race-a-global-view-of-gdpr-progress-in-the-united-states-europe-china-and-japan [https://perma.cc/Z9N8-QBX7].

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."[108] 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."[109] Several of the studies are based on surveys of selected participants, which of course reflect both who is invited to take them and who actually completes them.[110]

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. Data minimization or purpose specification may mean that companies do not gather data that they did not realize would prove useful for future business.[111] At the same time, however, gathering excessive amounts of information increases the risk of harm from any cybersecurity breach, as well as reputational risk.[112] Little information is available on the costs of restructuring of operations by businesses to bring themselves into compliance.

We conducted a survey among privacy experts to seek to obtain information about the costs of compliance for private enterprises.[113] The survey was circulated to privacy professionals both directly and through online social platforms, and was open for responses from June 18 to Au-

108. Ravi Sarathy & Christopher J. Robertson, *Strategic and Ethical Considerations in Managing Digital Privacy*, 46 J. BUS. ETHICS 111, 120 (2003).

109. PONEMON INST., THE TRUE COST OF COMPLIANCE WITH DATA PROTECTION REGULATIONS 4 (Dec. 2017), [hereinafter PONEMON INST., THE TRUE COST OF COMPLIANCE] https://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf [https://perma.cc/T3YF-4433].

110. *See id.* at 3; INT'L ASS'N PRIV. PROS., *supra* note 106, at iv; PONEMON INST., KEEPING PACE, *supra* note 107, at 36.

111. Alan McQuinn & Daniel Castro, *The Costs of an Unnecessarily Stringent Federal Data Privacy Law*, INFO. TECH. & INNOVATION FOUND. (Aug. 5, 2019), https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law [https://perma.cc/X4BV-DC78].

112. Sheryl Falk, Dan Roffman & Steve McNew, *Minimizing Privacy Risk with Data Minimization*, CORP. COUNS. (Sept. 2, 2019), https://www.law.com/corpcounsel/2019/09/02/minimizing-privacy-risk-with-data-minimization/?slreturn=20210530031228 [https://perma.cc/GML6-HAA8].

113. The complete survey and its results are posted online. Anupam Chander, Meaza Abraham, Sandeep Chandy, Yuan Fang, Dayoung Park & Isabel Yu, Default Report: World Bank Data Protection Survey (Aug. 3, 2020), https://drive.google.com/file/d/1CwzneOtePmmj0kZt7HBF-bxRkVfsORYc/view?usp=sharing [https://perma.cc/6M8U-N2QY].

gust 3, 2020. Various selection biases in our survey suggest caution 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 compliance 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 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 fifty-one responses to our survey from persons based in seventeen different countries. The top countries among our respondents were the United States (43%), India (11%), Germany (7%), and the United Kingdom (7%). Half of the respondents were consultants that help other organizations manage their data and 36% were data controllers themselves. The large majority of the respondents (81%) had no foreign ownership, while 13% of the respondents had less than 50% foreign ownership, and 6.38% of them had 50% or more foreign ownership. The percentage of respondents having more than 500 full-time employees was 41%; 17.39% of respondents had more than fifty and fewer than 500 full-time employees; 19.57% of respondents had more than ten and fewer than fifty full-time employees; and for 21.74% of respondents, the number of full-time employees was between one and ten. 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 our survey results or interviews as dispositive. The survey results and interviews have informed our study but largely 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 from July 2018 to April 2019.[114] Expenditures on activities and resources associated with

114. PONEMON INST., COST OF A DATA BREACH 3 (2019), [hereinafter PONEMON INST., COST OF A DATA BREACH] https://www.ibm.com/downloads/cas/RDEQK07R [https://perma.cc/TDF2-2J5M].

breaches with lifecycles of more than 200 days were $4.56 million.[115] An average of $0.21 million was expended on resources enabling organizations to notify regulators, such as the GDPR's Supervisory Authorities, and to inform affected data subjects of the relevant breach.[116] Another Ponemon Institute survey found that data breaches were widespread among the companies surveyed: "About half of the respondents had GDPR data breaches that must be reported to regulators."[117] This was consistent across the world: "Thirty-nine percent 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."[118]

A. Compliance Costs for E.U. Data Protection Law

1. Overall Costs of GDPR Compliance

As indicated earlier, estimates for average annual GDPR compliance costs 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.[119] 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 expenditure 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 in 2019.[120] That study was not restricted to companies complying with the GDPR alone, but surveyed companies across the world, including many in the United States.[121] Research focused on GDPR compliance conducted by the Ponemon Institute in 2019 on behalf of international law firm McDermott Will & Emery LLP (MW&E) found substantially higher figures: the average 2019 budget for GDPR activities was $13.6 million, a slight increase from $13.2 million in 2018.[122] A high percentage of the costs (between one-fifth and one-half, depending on the study) are associated with the hiring of privacy compliance personnel.[123] Technology also accounts for a significant portion (between 12% to 17%, depending on the study) of GDPR privacy expenses.[124] Outside consultants and lawyers accounted for another 18% to 20%, again de-

115. *Id*. at 34–35.
116. *Id.*
117. Ponemon Inst., Keeping Pace, *supra* note 107, at 2.
118. *Id.*
119. *See* Joseph Johnson, *Average Estimated GDPR Costs for FTSE100 Companies in the United Kingdom (UK) in 2018, by Sector*, STATISTA (Nov. 5, 2020), https://www.statista.com/statistics/869613/gdpr-implementation-cost-by-sector [https://perma.cc/Q7QS-MF4W].
120. Int'l Ass'n Priv. Pros, *supra* note 106, at 28.
121. *See id.* at 2.
122. Ponemon Inst., Keeping Pace, *supra* note 107, at 27.
123. *Id.* at 28; Int'l Ass'n Priv. Pros., *supra* note 106, at 39.
124. Ponemon Inst., Keeping Pace, *supra* note 107, at 28; Int'l Ass'n Priv. Pros., *supra* note 106, at 39.

pending on the study.[125] 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.[126]

The different results suggest 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, to $26 million for technology and telecommunications firms, and to $6 million for industrial goods and services firms.[127] Notably, despite these expenditures, most respondents (62% in the IAPP/EY study) believed their privacy budget was insufficient to meet their data protection obligations.[128] The cost of data privacy compliance can be quite high—so high that companies avoid certain jurisdictions entirely or simply ignore the laws.[129] More than half of the E.U. privacy professionals surveyed in the IAPP/EY study said that their organizations were not "fully" or even "very" compliant.[130]

The IAPP/EY study surveyed 370 respondents, predominately composed of organizations headquartered in the United States (39%), the European Union (33%), and the United Kingdom (13%).[131] Company size ranged from under 100 to over 75,000 employees, and represented industry sectors included technology, finance, healthcare, government, and consulting services.[132] The salaries and benefits of an organization's privacy team constituted the majority of privacy spending, receiving $397,100 on average; combined technology expenditures followed, receiving an average mean privacy spend of $172,000.[133] 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 $257,700 in 2019, whereas organizations with 75,000 or more employees had an estimated mean privacy expenditure of $1,883,200.[134]

125. PONEMON INST., KEEPING PACE, *supra* note 107, at 28; INT'L ASS'N PRIV. PROS., *supra* note 106, at 39.

126. DATAGRAIL, THE AGE OF PRIVACY: THE COST OF CONTINUOUS COMPLIANCE 6 (2020), https://datagrail.io/downloads/GDPR-CCPA-cost-report.pdf [https://perma.cc/RLU7-RYAT].

127. Johnson, *supra* note 119. Currency conversion from British pounds using XE.

128. INT'L ASS'N PRIV. PROS., *supra* note 106, at 37.

129. *See* Richard Stiennon, *Unintended Consequences of the European Union's GDPR*, FORBES (Nov. 27, 2017, 6:26 PM), https://www.forbes.com/sites/richardstiennon/2017/11/27/unintended-consequences-of-the-european-unions-gdpr/?sh=4d9466243c14 [https://perma.cc/8ZP7-LXM3].

130. INT'L ASS'N PRIV. PROS., *supra* note 106, at iv.

131. *Id.* at viii, 2.

132. *Id.* at 3–4.

133. *Id.* at 28.

134. *Id.* at 30.

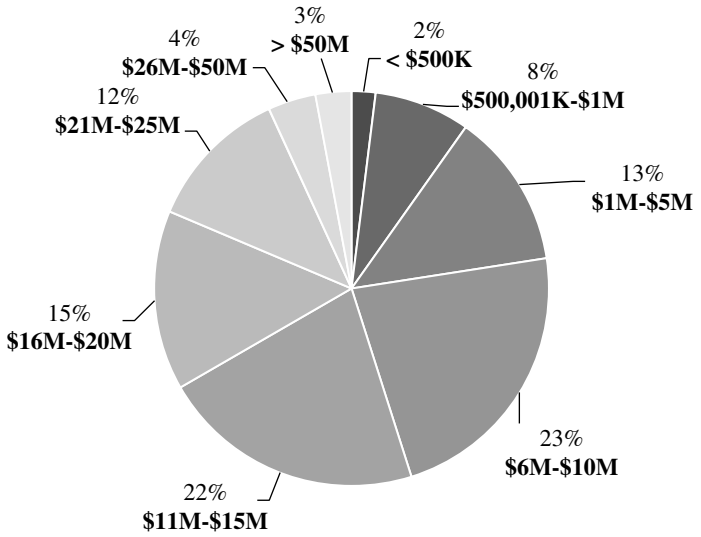
FIGURE 1: MEAN 2019 ESTIMATED PRIVACY SPEND REPORTED TO IAPP BY EMPLOYEE SIZE, U.S. DOLLARS[135]

Category	**<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
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 MW&E.[136] Respondents hailed from the United States (544), Europe (371), China (102), and Japan (246).[137] Represented organizations ranged from those with fewer than 500 employees to those with over 75,000 employees, and predominant industries were financial services (18%), industrial (13%), entertainment (11%), and health and pharmaceuticals (11%).[138] The survey found an average GDPR compliance budget of $13.6 million in fiscal year 2019.[139]

135. *Id.*
136. PONEMON INST., KEEPING PACE, *supra* note 107, at 2.
137. *Id.* at 31.
138. *Id.* at 38.
139. *Id.* at 27.

FIGURE 2: ANNUAL BUDGETS FOR GDPR COMPLIANCE IN 2019, U.S. DOLLARS[140]



2. Components of GDPR Compliance

The studies shed light on the various components of the costs of compliance. Managed services, personnel, and technologies continued to receive the greatest amount of funding, experiencing few to no changes in allocation since 2018.[141]

140. *Id.* at 62.
141. *Id.* at 28.

FIGURE 3: DISTRIBUTION OF PRIVACY BUDGET, 2018–2019[142]

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%

The large expenditure in banking may be the result of the high risk posed by banks' 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.[143]

142. *Id.*; INT'L ASS'N PRIV. PROS., *supra* note 106 at 39.

143. Abi Millar, *GDPR: How Is It Affecting Banks?*, FIN. DIR. (June 21, 2018), https://www.financialdirector.co.uk/2018/06/21/gdpr-how-is-it-affecting-banks [https://perma.cc/4SXN-577V].

FIGURE 4: TOTAL COMPLIANCE COST FOR FTSE 100 COMPANIES, MILLIONS OF U.S. DOLLARS[144]

The figures in the table below have been converted from GBP to USD using XE's currency converter and were rounded.

Research Entity	**Industry**	**Cost of GDPR Compliance**
Statista, 2018	Banks	$93.8M
	Technology & Telecoms	$28.5M
	Energy & Utilities	$27.3M
	Retail	$21.4M
	Healthcare	$15.4M
	Travel & Leisure	$14.2M
	Financial Services	$11.3M
	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
	Healthcare	$19M
	Pharmaceuticals	$18.2M
	Consumer Products	$17.6M
	Communications	$16.7M
	Public Sector	$14.5M
	Retail	$11.5M
	Education & Research	$9.8M
	Media	$7.7M

Salaries for privacy compliance personnel form a major part of privacy-related expenditures.[145] A study by DataGrail surveyed 301 professionals involved in the GDPR decision-making process at companies with fifty or more employees in 2019 and found that 67% of companies engaged at least twenty-five employees when preparing for the GDPR; 44% of companies had at least fifty employees.[146] Findings from the IAPP's survey

144. Johnson, *supra* note 119; PONEMON INST., THE TRUE COST OF COMPLIANCE, *supra* note 109, at 10.

145. *See* INT'L ASS'N PRIV. PROS., *supra* note 106, at 28.

146. DATAGRAIL, *supra* note 126, at 3.

showed that privacy staffing, like total privacy spending on GDPR compliance, reportedly leveled off in 2019: only 30% of organizations surveyed in 2019 expected an increase in full-time privacy staff, 66% expected no changes, and 4% expected a decrease.[147] A mean of 7.1 employees work on privacy-related matters full-time while a mean of 15.7 do so part-time.[148]

FIGURE 5: STAFF-RELATED PRIVACY EXPENDITURES[149]

The figures in the table below have been converted from euros to U.S. dollars using XE's currency converter and were rounded.

Research Entity	**Staff Related Expenditure**	**Cost**
IAPP-EY, 2019 (Respondents: 370 privacy professionals from the IAPP database located in the United States and the European Union)	Privacy Team Salaries and Benefits (2019)	$397,100 (average)
	Salary and Travel (2018)	47% of privacy budget
	Salary and Travel (2019)	50% of privacy budget
Paul Hastings, 2017 (Respondents: 100 FTSE 350 firms in the United Kingdom and 100 Fortune 500 companies in the United States)	Additional Staff (United Kingdom)	40% of respondents have allocated $263,600–$524,700
	Additional Staff (United States)	34% of respondents have allocated $501,000–$1M

Data from MW&E's study reported that almost half of the organizations represented (48%) are in the process of hiring or are expecting to hire an average of almost four additional employees to provide ongoing assistance with the GDPR.[150] 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.[151]

147. INT'L ASS'N PRIV. PROS., *supra* note 106, at 27.

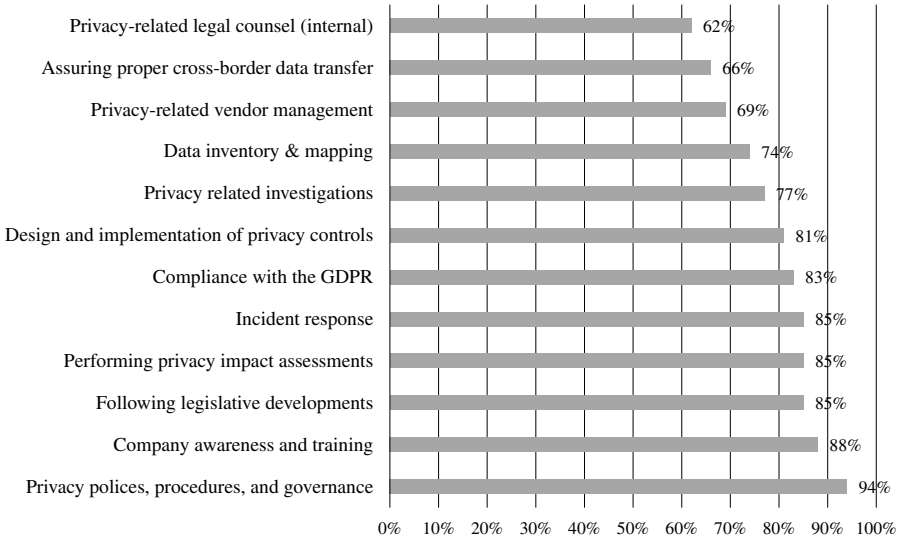
148. *Id.* at 23.

149. *Id.* at 28; *Fortune and FTSE Firms to Spend Millions Gearing Up for GDPR Compliance, New Survey Shows*, PAUL HASTINGS (Oct. 25, 2017), https://www.paulhastings.com/news/news-fortune-and-ftse-firms-to-spend-millions-gearing-up-for-gdpr-compliance-new-survey-shows [https://perma.cc/X7SK-T9V5].

150. PONEMON INST., KEEPING PACE, *supra* note 107, at 27.

151. *Id.* at 25.

FIGURE 6: PRIVACY TEAM RESPONSIBILITIES REPORTED TO IAPP-EY, 2019[152]



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 may require configuration of their databases.[153] According to DataGrail's survey findings, 58% of companies had received eleven or more data subject requests (DSRs) per month since the GDPR's implementation and the survey's closing in April 2019, and 28% received 100 or more per month.[154] A reported 58% of companies had at least twenty-six employees processing a single data subject request in 2018; this can likely be attributed 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.[155]

152. INT'L ASS'N PRIV. PROS., *supra* note 106, at 42–43.

153. Rita Heimes, *Top 10 Operational Responses to the GDPR—Part 1: Data Inventory and Mapping*, INT'L ASS'N PRIV. PROS. (Feb. 1, 2018), https://iapp.org/news/a/top-10-operational-responses-to-the-gdpr-data-inventory-and-mapping [https://perma.cc/U6ZQ-FLAR].

154. DATAGRAIL, *supra* note 126, at 8.

155. *See id.* at 2, 8.

FIGURE 7: OPERATIONAL COSTS OF MANAGING DATA SUBJECT REQUESTS: VOLUME OF DATA SUBJECT REQUESTS RECEIVED PER MONTH SINCE APRIL 2019[156]

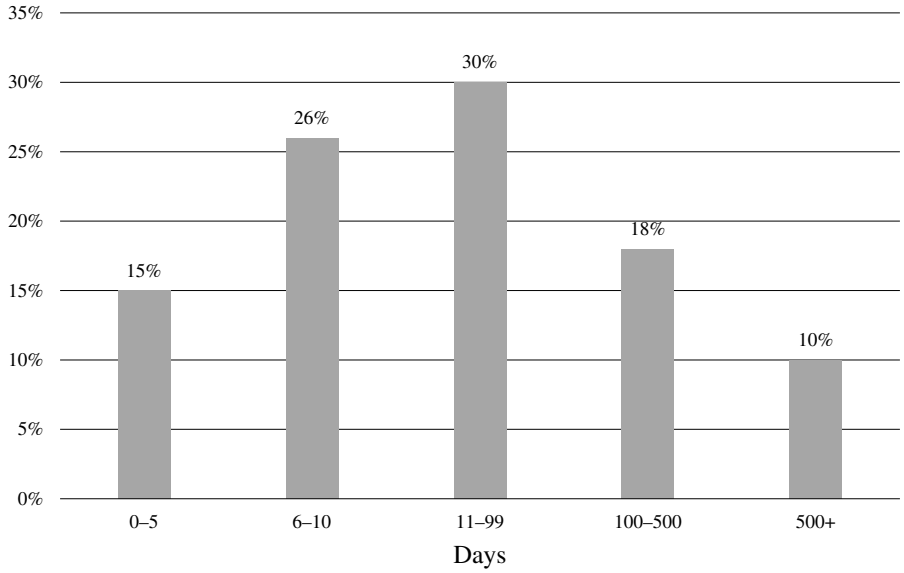
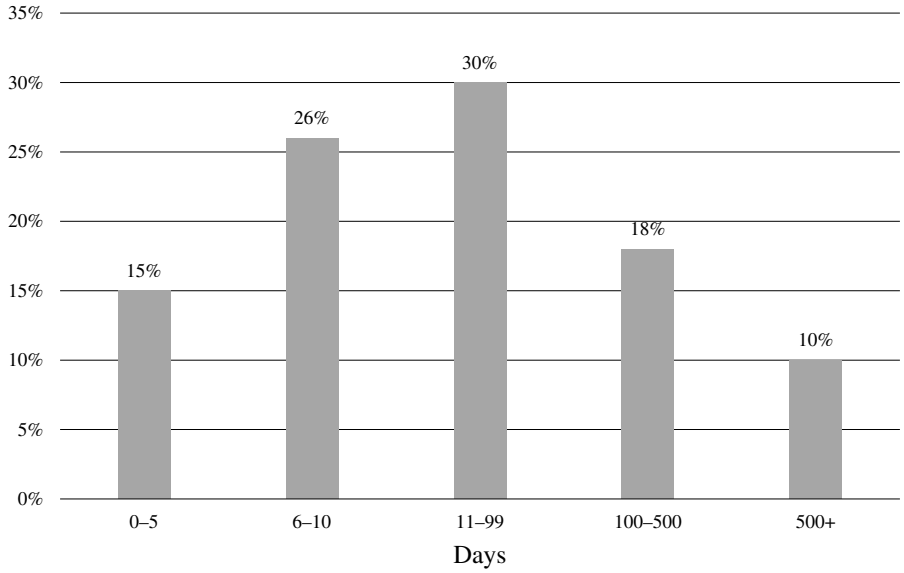


FIGURE 8: OPERATIONAL COSTS OF MANAGING DATA SUBJECT REQUESTS: NUMBER OF EMPLOYEES INVOLVED IN PROCESSING A SINGLE DATA SUBJECT REQUEST SINCE APRIL 2019[157]



156. *Id.* at 8.
157. *Id.*

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.[158] A data subject request imposes a range of duties: from locating, compiling, and providing a data subject with all the information an organization has stored on the subject, free of charge, which is commonly known as "the "right of access,"[159] to locating and deleting all the information stored on a data subject, which is known as the "right to be forgotten."[160] The challenges posed by data subject requests were echoed by the IAPP's study in which 56% of the 370 surveyed organizations reported "locating unstructured personal data" as "difficult."[161]

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.[162] 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 processing were present; and an excess of 25,000 employees or revenue exceeding $25 billion.[163] IAPP respondents that received higher levels of data subject requests reported that they experienced less difficulty managing requests than respondents who received fewer data subject requests.[164] 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.[165]

Though an organization is only required to hire a Data Protection Officer when (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,[166] studies suggest many organizations have heeded the GDPR's encouragement to appoint a Data Protection Officer even when they are not required to do so. An overwhelming 92% of MW&E's 1,263 respondents[167] and three-fourths of the IAPP's 370 respondents[168] appointed Data Protection Officers despite both surveys including a wide variety of organizations that, per the GDPR criteria, are not required to appoint a Data Protection Officer.[169] Most organizations have appointed only one Data Protection Officer, though

158. *See id.* at 4; GDPR, *supra* note 23, arts. 12, 15.
159. GDPR, *supra* note 23, arts. 12, 15.
160. *Id.* art. 17.
161. INT'L ASS'N PRIV. PROS., *supra* note 106, at v.
162. *See id.* at xiv, xx.
163. *Id.*
164. *Id.* at xix, 89.
165. *Id.* at xix, 95.
166. GDPR, *supra* note 23, art. 37.
167. PONEMON INST., KEEPING PACE, *supra* note 107, at 21, 36.
168. INT'L ASS'N PRIV., *supra* note 106, at iv.
169. PONEMON INST., KEEPING PACE, *supra* note 107, at 3; INT'L ASS'N PRIV. PROS., *supra* note 106, at iv, 6.

18% of organizations have expended resources on appointing multiple.[170] 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.[171]

MW&E's 2019 study found that 46% of respondents had hired outside counsel for GDPR compliance.[172] The survey found that 68% of organizations hired outside counsel to conduct data protection impact assessments,[173] a time- and labor-intensive procedure performed whenever a processing activity using new technologies is proposed and required of organizations engaging in high-risk processing.[174] 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.[175] Approximately 34% of respondents sought outside counsel for assistance with international data transfers.[176] The invalidation of the E.U.–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.[177]

FIGURE 9: PERCENT OF BUDGET ALLOCATED FOR OUTSIDE COUNSEL & CONSULTING SERVICES[178]

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%
	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 respon-

170. INT'L ASS'N PRIV. PROS., *supra* note 106, at xii.

171. Oliver Smith, *The GDPR Racket: Who's Making Money From this $9bn Business Shakedown*, FORBES (May 2, 2018, 2:30 AM), https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/?sh=3fe8cf7934a2 [https://perma.cc/4NG5-YE38].

172. PONEMON INST., KEEPING PACE, *supra* note 107, at 23.

173. *Id.* at 24.

174. GDPR, *supra* note 23, art. 35.

175. PONEMON INST., KEEPING PACE, *supra* note 107, at 60.

176. *Id.*

177. INT'L ASS'N PRIV. PROS., *supra* note 106, at xix; *see also* Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd., ECLI:EU:C:2020:559 (July 16, 2020).

178. PONEMON INST., KEEPING PACE, *supra* note 107, at 28; INT'L ASS'N PRIV. PROS., *supra* note 106, at xx.

dents reporting that their processing was outsourced.[179] The GDPR mandates that personal data should be outsourced to third parties for processing only when those processors provide sufficient guarantees through a written contract that processing will occur in accordance with the GDPR.[180] Data controllers remain responsible for noncompliance by the processors with which they share data.[181] 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.[182] 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.[183]

The GDPR does not outline specific technologies that organizations should use, though the use of encryption and pseudonymization are encouraged and required whenever feasible.[184] The IAPP found an average of $172,000 was spent on technology expenditures.[185] 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.[186] The MW&E study produced similar results: from a surveyed pool of 1,263 privacy professionals, 46% respondents invested in new technologies or services in preparation for GDPR compliance.[187]

179. INT'L ASS'N PRIV. PROS., *supra* note 106, at iv.
180. GDPR, *supra* note 23, art. 28.
181. *Id.* art. 82.
182. INT'L ASS'N PRIV. PROS., *supra* note 106, at xv–xvi.
183. *Id.* at xvi.
184. GDPR, *supra* note 23, art. 32.
185. *See* INT'L ASS'N PRIV. PROS., *supra* note 106, at 28.
186. DATAGRAIL, *supra* note 126, at 5, 12.
187. PONEMON INST., KEEPING PACE, *supra* note 107, at 21, 36.

FIGURE 10: COMPANY SPENDING ON CONSULTING SERVICES AND/OR TECHNOLOGY IN PREPARATION FOR GDPR COMPLIANCE[188]

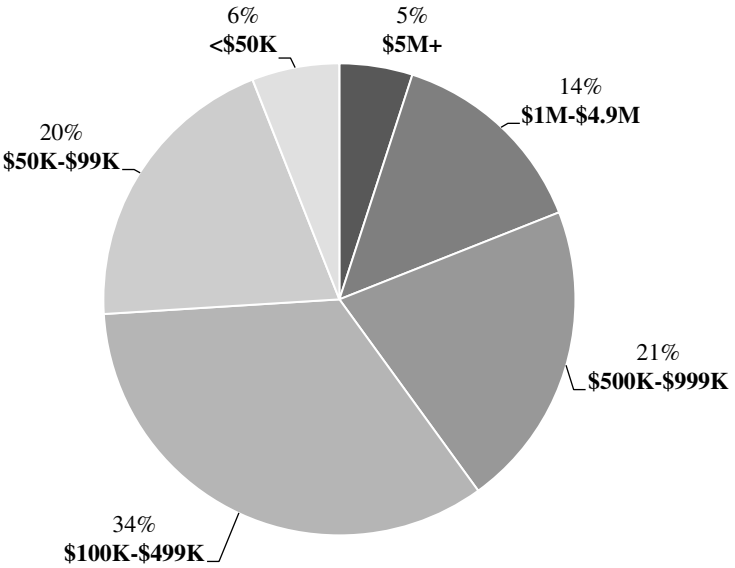


FIGURE 11: MANUAL VERSUS AUTOMATION: TOOLS AND METHODS USED BY ORGANIZATIONS FOR GDPR COMPLIANCE[189]

Tools Used for Data Inventory and Mapping	Email, spreadsheets, in-person communication (manual)	60%
	Commercial software tool designed for data inventory/mapping	31%
	System developed internally	30%
	Data Loss Prevention (DLP) technology	21%
	GRC software customized in-house for inventory/mapping	20%
	Outsource data inventory/mapping to external consultants/law firms	8%
	Don't know	4%
Method for Handling Data Subject Requests	Entirely manual	64%
	Partially automated	25%
	Still being designed	7%
	Haven't yet addressed	2%

188. DATAGRAIL, *supra* note 126, at 5.
189. INT'L ASS'N PRIV. PROS., *supra* note 106, at 62, 64.

Of the 1,263 organizations surveyed by MW&E, 31% of respondents purchased insurance covering cyber risks.[190] Of those insured, 43% had insurance coverage for GDPR fines and penalties.[191] Expenditures on cybersecurity insurance varied 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.[192] Data breach disclosure requirements continue to be a challenge for many organizations; only 18% of MW&E's respondents said they were confident in their ability to notify a data protection authority within seventy-two hours of becoming aware of the incident, as required by the GDPR.[193] The study suggests that many organizations will need to spend additional funds on external cybersecurity services that would enable them to identify cyberattacks early on and to provide data protection authorities the necessary forensic evidence within the mandated window of time.[194]

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.[195] For the largest companies, this could result in fines in the millions or even billions of dollars.[196] 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.[197] As of August 5, 2021, there have been approximately 735 instances where fines have been imposed on organizations under the GDPR.[198]

B. Compliance Costs for U.S. Privacy Law

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

1. HIPAA Compliance Costs

Studies over the last two decades have estimated that the health industry as a whole spends billions of dollars on HIPAA compliance initiatives. In 1999 and 2000, healthcare consulting companies estimated the cost for

190. Ponemon Inst., Keeping Pace, *supra* note 107, at 52.
191. *Id.* at 53.
192. *Id.* at 35–36.
193. *Id.* at 10.
194. *See id.*
195. GDPR, *supra* note 23, art. 83.
196. Stiennon, *supra* note 129.
197. GDPR, *supra* note 23, art. 33. No such notification is required if the data breach is unlikely to present a risk to the rights and liberties of data subjects or notification within seventy-two hours is rendered unfeasible by circumstance. *Id.*
198. *Fines Statistics*, CMS, https://www.enforcementtracker.com/?insights [https://perma.cc/F67L-JSVR].

compliance to total from $25 billion to $43 billion in the first five years.[199] DHHS, 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.[200] In 2003, the research firm Gartner Group estimated that the healthcare industry would spend between $3.8 billion and $38 billion in pursuit of HIPAA compliance from 2003 to 2008.[201]

For individual healthcare 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.[202] 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.[203] 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."[204]

FIGURE 12: COST OF HIPAA COMPLIANCE FOR THE INDUSTRY[205]

Research Entity	**Affected Respondents**	**Estimated Cost of Compliance**
Healthcare Consulting Companies (2003)	Healthcare providers (covered entities)	$25–$43 billion (first 5 years)
DHHS (2002)	Healthcare providers (covered entities)	$3.2 billion (first year) $17.6 billion (first 10 years)
Gartner Group (2003)	Entire healthcare industry	$3.8–$38 billion (2003-2008)

In 2011, after certain HIPAA modifications, the DHHS conducted a study to estimate the additional cost of compliance imposed by the modifications.[206] DHHS surveyed "covered entities," which include all health plans, healthcare clearinghouses, and healthcare providers.[207] DHHS estimated the additional costs incurred to be between $114 million and $225.4 million in the first year of implementation and approximately

199. Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 132 & n.239 (2002).
200. *Id.* at 132.
201. KEVIN BEAVER & REBECCA HEROLD, THE PRACTICAL GUIDE TO HIPAA PRIVACY AND SECURITY COMPLIANCE 23 (2004).
202. *Id.* at 24.
203. *Id.*
204. *Id.*
205. Hahn & Layne-Farrar, *supra* note 199, at 132–33; REBECCA HEROLD & KEVIN BEAVER, THE PRACTICAL GUIDE TO HIPAA PRIVACY AND SECURITY COMPLIANCE 46 (2014).
206. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566, 5566 (Jan. 25, 2013).
207. *Id.* at 5567.

$14.5 million annually thereafter.[208] These costs include: (1) costs to HIPAA covered entities to revise and distribute updated notices of privacy practices; (2) costs to HIPAA covered entities to comply with the requirements of breach notification; (3) costs to business associates to ensure their subcontracts are complying with business associate agreement requirements; and (4) costs to business associates to fully comply with HIPAA's Security Rule.[209]

The tables that follow break down the estimated costs that covered entities and their business associates expend per year to comply with HIPAA's modified provisions.

FIGURE 13: ESTIMATED COSTS FOR HIPAA COMPLIANCE[210]

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

208. *Id.*
209. *Id.*
210. *Id.* at 5567, 5676.

FIGURE 14: ANNUAL COMPLIANCE COSTS FOR NOTICE OF PRIVACY PRACTICES[211]

Legislation	**Affected Respondents**	**Cost of Compliance (USD/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	

FIGURE 15: ANNUAL COMPLIANCE COSTS FOR BREACH NOTIFICATION[212]

Total Cost of Compliance (USD/year) for 698,238 Covered Entities	**Cost of Compliance Components**
$3,467,122	E-mail and First Class Mail, which includes the cost to compose and document notice, the hours and cost to prepare mailing, and the cost of necessary postage and supplies
$571,200	Substitute Notices: Media Notice
$1,816,379	Substitute Notices: Toll-free Number, which 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
$422,438	Annual Report to the Secretary: Under 500
Total Costs	$14,475,600/year

211. *Id.* at 5676.
212. *Id.* at 5671.

2. GLBA Compliance Costs

Robert Hahn and Anne Layne-Farrar's 2002 study detailed the industry-wide cost of compliance with the GLBA.[213] The study found that banking, insurance, and securities companies altogether may spend around $2–$5 billion on printing costs alone to comply with the regulation's privacy policy notifications.[214] In 2016, nearly fifteen years after Hahn and Farrar's study, amendments to the GLBA created exceptions to the annual privacy notice requirements.[215] The Bureau of Consumer Financial Protection calculated that the modified privacy notice procedures decreased costs by $3 million per institution.[216]

213. *See generally* Hahn & Layne-Farrar, *supra* note 199.
214. *Id.* at 145.
215. Amendment to the Annual Privacy Notice Requirement Under the Gramm–Leach–Bliley Act, 83 Fed. Reg. 40945, 40945 (Aug. 17, 2018) (to be codified at 12 C.F.R pt. 1016).
216. *Id.* at 40956.

FIGURE 16: ESTIMATED COST OF GLBA COMPLIANCE BEFORE AND AFTER AMENDMENTS[217]

Legislation	**Estimating Entity**	**Affected Respondents**	**Cost of Compliance Components**	**Cost of Compliance (USD/year)**
GLBA	Fred H. Cate and FleetBoston Financial Corporation	Banking, insurance, and securities companies (surveyed 40,000 financial institutions)	Printing costs for all privacy policy notifications	$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	Bureau of Consumer Financial Protection	Banks, credit unions and non-depository financial institutions. (surveyed 19 banks with assets over $100 billion; 106 additional banks selected through random sampling)	Cost of annual privacy notice	$12 million (pre-amendment)–$3 million (savings from amendment) = $9 million per institution Reduction in burden (per bank) = $3 million/year Reduction in burden (per non-depository financial institution) = $231,000/year

217. *Id.*; Hahn & Layne-Farrar, *supra* note 199, at 145; Fred H. Cate, Professor of Law, Indiana University School of Law, The Privacy Paradox, Prepared Statement at 76th Annual Winter Newspaper Institute, Address Before North Carolina Press Association (Jan. 26, 2001) ("Approximately 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 GLBA.).

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 that the cost of compliance with COPPA ranged from $115,000 to $290,000 per year for a mid-sized children's website, depending on the nature of the site.[218] The House Committee broke down the costs as indicated in the table below.[219] Both the compliance activities and the actual compliance costs are likely to be significantly different than those estimated by Congress two decades ago.

FIGURE 17: BREAKDOWN OF ESTIMATED COPAA COMPLIANCE COSTS IN 2000[220]

COPPA Compliance 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)	$2,500–$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

Instead of complying with the legislation, some companies have sought to avoid COPPA altogether by excluding children under thirteen from their consumer base.[221]

218. *Recent Developments in Privacy Protections for Consumers: Hearing Before the Subcomm. on Telecomm., Trade, and Consumer Prot. of the Comm. on Com.*, 106th Cong. 83 (2000) [hereinafter *Recent Developments in Privacy Protections for Consumers*] (statement of Parry Aftab, Special Counsel, Darby & Darby, P.C.).

219. *See id.* 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 FTC, 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?* LEXOLOGY (Jul. 26 2013), https://www.lexology.com/library/detail.aspx?g=0b6d68a9-5d17-4d52-9b30-54d356ddb08a [https://perma.cc/6549-HCY4].

220. *Recent Developments in Privacy Protections for Consumers*, *supra* note 218, at 83 (statement of Parry Aftab, Special Counsel, Darby & Darby, P.C.).

221. *See* Manatt Phelps & Phillips LLP, *supra* note 219.

C. Compliance in China

We were unable to locate studies on the costs of private sector compliance with China's data privacy regime. Discussions with Chinese privacy law experts suggest that costs are high due to numerous privacy guidelines or rules, uncertainties regarding the obligations, and possible requirements for data localization.

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.[222] 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.[223] Remedies can include "warnings, orders to rectify, fines, . . . compensation to victims," and even prison sentences.[224] While the GDPR permits fines up to 2% of a company's global annual revenue[225]—an amount that can be in the billions of dollars for large companies—the fines available under Chinese law are relatively low and allow a maximum fine of approximately RMB 1,000,000 (about $141,000).[226] Authorities may seek sanctions against responsible personnel and revoke their licenses to operate, resulting in the shutdown of an app or website entirely—a remedy even more serious than financial penalties.[227]

Over the last two years, 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 one thousand apps for data practices and requiring subsequent changes from many of them.[228] 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, and reportedly shut down

222. Tianshu Sun, Zhe Yuan, Chunxiao Li, Kaifu Zhang & Jun Xu, *The Value of Personal Data in Internet Commerce: A High-Stake Field Experiment on Data Regulation Policy* (Univ. S. Cal., Working Paper No. 3566758, 2020), https://privpapers.ssrn.com/sol3/papers.cfm?abstract_id=3566758 [https://perma.cc/L6G5-RAAM].

223. DLA Piper, Data Protection Laws of the World 163 (2021), https://www.dlapiperdataprotection.com [https://perma.cc/JT7P-4D7R].

224. *Id.*

225. *What Are the GDPR Fines?*, GDPR.EU, https://gdpr.eu/fines [https://perma.cc/Q6PA-PD3Y].

226. Gil Zhang & Kate Yin, *A Look at China's Draft of Personal Information Protection Law*, IAPP (Oct. 26, 2020), https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law [https://perma.cc/PHK4-SD6G].

227. *See* Jenny (Jia) Sheng, Chunbin Xu & Esther Tao, *China Adopts New Data Security Law*, Pillsbury (July 9, 2021), https://www.pillsburylaw.com/en/news-and-insights/china-adopts-new-data-security-law.html [https://perma.cc/SRC2-TYR9].

228. Dai & Deng, *supra* note 98, at 15.

around 33,638 apps that were found to possess illicit content.[229]

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 through audits may be construed as part of a broader effort to ensure control of information circulated online and thus as part of a national security effort.[230]

In 2019, China's National Information Security Standardization Technical Committee proposed revisions to the 2018 Specification, calling for companies to appoint a person or office to oversee data collection if the company either (1) employs more than two hundred people to process personal data or (2) processes data for more than one million people over the span of twelve months.[231] 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.[232] For instance, tech companies such as WeChat, ByteDance, and Tencent have initiated civil disputes against their competitors in court, aiming to prevent access to protected information.[233] In the past few years, ordinary citizens have increasingly taken advantage of this system to fight tech companies in pursuit of their own privacy rights.[234] Private costs of compliance can also be inferred from the Cybersecurity Law penalty system. When companies fail to comply with the 2017 Cybersecurity Law, they are subject to fines from 100,000 to 1,000,000 RMB ($14,351–$143,517).[235]

Like the GDPR, the Cybersecurity Law applies to businesses and organizations in all industries; however, several sectors in the private sector have additional requirements regarding data protection and privacy.[236] Within the life sciences industry, China focuses most of its regulation efforts on localizing healthcare data and scientific research through legislation such as the Measures for the Management of Scientific Data and the Measures for the Management of Population Health Information.[237]

The People's Bank of China led regulatory efforts within the financial industry when it published the Implementation Measures for Protecting Financial Consumers' Rights and Interests in December 2019 and effectuated the Personal Financial Information Protection Technical Specifica-

229. *Id.* at 16.

230. *See generally* Anupam Chander, *Googling Freedom*, 99 CALIF. L. REV. 1 (2010).

231. Gil Zhang & Kate Yin, *More Updates on the Chinese Data Protection Regime in 2019*, IAPP (Feb. 26, 2019), https://iapp.org/news/a/more-positive-progress-on-chinese-data-protection-regime-in-2019 [https://perma.cc/8FQU-6X3H].

232. DAI & DENG, *supra* note 98, at 20.

233. *Id.* at 3, 20–21.

234. *Id.* at 20–21.

235. KPMG CHINA, WANGLU ANQUANFA GAILAN (网路安全法概览) 6 (2017), https://assets.kpmg/content/dam/kpmg/cn/pdf/zh/2017/02/overview-of-cybersecurity-law.pdf [https://perma.cc/3GRH-ZCKF].

236. *See* DAI & DENG, *supra* note 98, at 23.

237. *Id.* at 24–25.

tion in February 2020.[238] The government published the National Standards on Information Security Technology in March 2020, which came into force in October 2020.[239] Because these regulations focus on protecting consumer financial information,[240] companies in the financial industry are encouraged to encrypt data and implement adequate access controls, and they must justify the purpose, method, and scope of their data collection.[241]

The Information Security Technology Personal Information Security Specification governs the e-commerce industry and includes regulations on how companies may store personal data and obtain consent from customers.[242] 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 maintain a data breach response plan.[243]

IV. 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 laws in Europe, the United States, and China.

This section aims to identify the financial and employee resources available to regulators and compare them to the enforcement actions undertaken by the regulators. Both E.U. and U.S. agencies publish this information annually. While China has actively enforced data security and privacy rules in the last two years, 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.[244] Unlike the GDPR and U.S. regulations, the Chinese data protection regime does not have a single regulator; 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.[245] Budgets for data protection enforcement were not readily available, so we limit our discussion to describing enforcement activities.

238. Chan, Yue & Ke, *supra* note 82.
239. *Id.*
240. DAI & DENG, *supra* note 98, at 27.
241. *Id.* at 27.
242. *Id.* at 28–29.
243. *Id.* at 29–30.
244. *See* Pernot-Leplay, *supra* note 61, at 82.
245. *Id.* at 90; *New Chinese Cybersecurity and Data Privacy Requirements*, JONES DAY (Dec. 2020), https://www.jonesday.com/en/insights/2020/12/new-chinese-cybersecurity-and-data-privacy-requirements [https://perma.cc/HT9P-DNGX].

Because this is a fast-changing area, any snapshot will not capture the full dynamics at play. Our review has made it clear that budgets for enforcement have not kept up with the regulations or the scope of the digital economy. 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.

While the United States lacks dedicated privacy agencies like those present in European countries, the FTC has levied significantly higher fines than E.U. data protection authorities.[246] Since May 2018, when the GDPR came into force, through the beginning of 2021, the FTC imposed $5.8 billion in total fines, while the European data protection authorities levied a total of $326 million.[247] That seems likely to change, as European authorities plan large fines for many American firms.[248]

A. Enforcement in the European Union

1. Overview

On average, the E.U. member states allocated €7 million to each of their data protection authorities in 2021.[249] At the high end, Germany allocated €94.7 million among both its federal and state data protection authorities, while Cyprus, Malta, and Estonia, allocated just €0.7 million, €0.6 million, and €0.8 million, respectively, for the latest year available.[250] Collectively, in 2021, the E.U. member states expended €301 million to enforce data privacy rules governing some 513 million people—less than a euro (or a dollar) per person for the year.[251]

The GDPR requires each member state to establish Data Protection Authorities (DPAs) with sufficient financial resources for their operations.[252] In addition to enforcing the GDPR, the DPAs raise awareness,

246. Mark Scott, *Digital Competition—Big Tech Down Under—Section 230's Dirty Secret*, Politico: Digital Bridge (Feb. 11, 2021), https://www.politico.eu/newsletter/digital-bridge/politico-digital-bridge-digital-competition-big-tech-down-under-section-230s-dirty-secret [https://perma.cc/9YXR-63WG].

247. *Id.*

248. *See* Ryan Browne, *Europe's Privacy Overhaul Has Led to $126 Million in Fines—But Regulators Are Just Getting Started*, CNBC (Jan. 19, 2020, 7:02 PM), https://www.cnbc.com/2020/01/19/eu-gdpr-privacy-law-led-to-over-100-million-in-fines.html [https://perma.cc/Z6LM-JERZ].

249. *See Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities*, Eur. Data Prot. Bd. (Aug. 2021) [hereinafter *Overview on Resources*], https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf [https://perma.cc/Y8AV-PW2A].

250. *See id.*; Johnny Ryan & Alan Toner, Brave, Europe's Governments are Failing the GDPR 6 (2020), https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf [https://perma.cc/7HB2-99K4] (vacancies included in count and full-time equivalents are rounded; data on Austria's tech specialists is unavailable).

251. *See* Ryan & Toner, *supra* note 250, at 6.

252. GDPR, *supra* note 23, arts. 51–52.

provide guidance, handle complaints, and conduct investigations.[253] The GDPR also imposes a duty of cooperation on member states.[254] The GDPR hoped to create a full service 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.[255] Secondary "concerned authorities" may also assist in the investigation.[256]

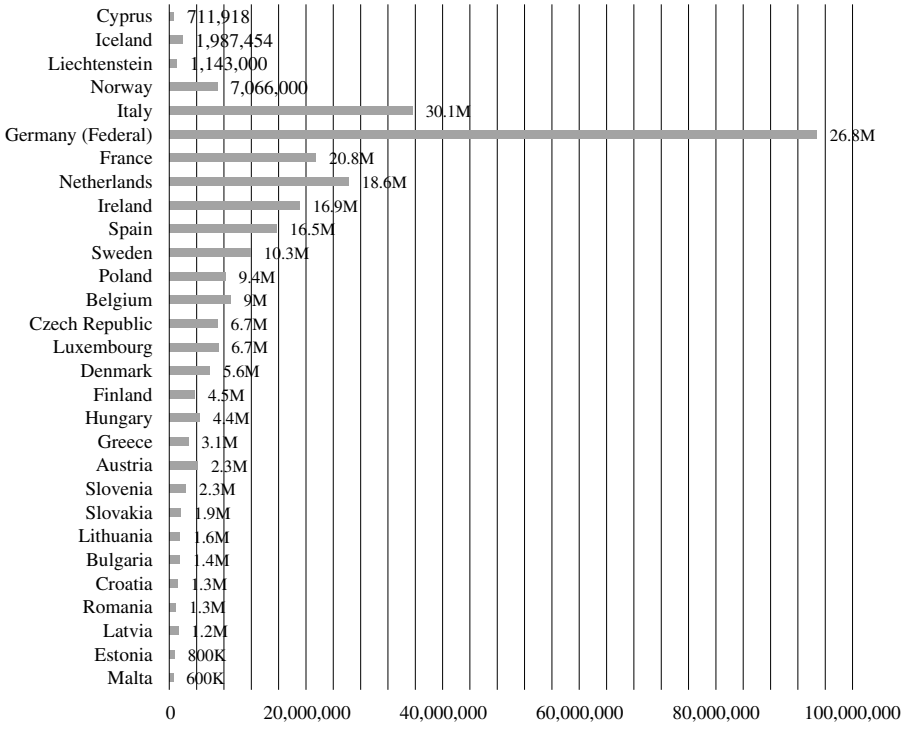
Budgets allocated to DPAs are generally increasing, although at significantly lower rates than the one-time jump observed between 2017 and 2018, the latter being the year when the GDPR went into effect.[257] Twenty-one out of the thirty DPAs surveyed by the European Data Protection Board (EDPB)[258] reported dissatisfaction with their level of resourcing.[259] 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.[260]

2. National Enforcement

Most European governments spend less than one euro per citizen per year on their data protection authority.[261] Many supervisory authorities complain of insufficient funding.[262] Despite such complaints, most DPAs expect budgets to remain static in the upcoming year.[263] 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.[264]

253. DELOITTE, REPORT ON EU DATA PROTECTION AUTHORITIES, PART 5: GUIDANCE ISSUED 2 (2019), https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/risk-reports-privacy-and-data-protection-guidance-issued.pdf [https://perma.cc/7JL8-U8HJ].
254. GDPR, *supra* note 23, art. 31.
255. *See id.* art. 56.
256. *Id.* art. 4(22).
257. *See* RYAN & TONER, *supra* note 250, at 6.
258. Under the GDPR, the European Data Protection Board is the working group made up of representatives from each E.U. member state's national DPA.
259. ACCESS NOW, TWO YEARS UNDER THE EU GDPR: AN IMPLEMENTATION PROGRESS REPORT 9 (2020), https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf [https://perma.cc/TQJ3-SQUD].
260. *See id.* at 9, 13.
261. *See* RYAN & TONER, *supra* note 250, at 6.
262. ACCESS NOW, *supra* note 259, at 9.
263. *Id.* at 10.
264. EUR. PARL. DOC. B9-0211/2021 ¶ 17 (2021).

FIGURE 18: 2021 DPA BUDGETS IN EUROS[265]



Using online forms and supplementary guidance procedures, data subjects and related organizations submit complaints to the DPAs, while data processors and controllers submit data breach notifications. [266] 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 E.U. member states.[267] Through IMI, DPAs can coordinate with the authorities of other concerned or lead member states by utilizing a series of pre-translated question-and-answer forms, while also tracking the case's development.[268] Complaints may also be lodged by the DPA itself pursuant to the investigative and super-

265. *See Overview on Resources*, *supra* note 249, at 4. Slightly different budget figures are reported in DELOITTE, REPORT ON EU DATA PROTECTION AUTHORITIES PART 4: RESOURCES (2019), https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-reports-resources.pdf [https://perma.cc/9D7B-GX34].

266. GDPR, *supra* note 23, art. 33; *Complaints*, EUR. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en [https://perma.cc/JM2Y-JPEX].

267. *See generally Internal Market Information System*, EUR. COMM'N, https://ec.europa.eu/internal_market/imi-net/index_en.htm [https://perma.cc/AM4V-Y92D]; *Our Members*, EUR. DATA PROT. BD., https://edpb.europa.eu/about-edpb/about-edpb/members_en [https://perma.cc/96HD-34V4].

268. *See Single Market Scoreboard*, EUR. COMM'N (2020), https://ec.europa.eu/internal_market/scoreboard [https://perma.cc/M3PR-RZ4U].

visory powers granted by the GDPR.[269]

The second and third year of GDPR implementation have seen a dramatic increase in the quantity of complaints received by member states. Since May 25, 2018, the German enforcement authorities alone received 66,965 and the French authorities received 41,601 complaints.[270] Each complaint requires processing by DPA employees and, if appropriate, an investigation to determine the complaint's validity.[271] 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 to respond to the influx of complaints received by overworked complaint handlers.[272] These approaches seek to offer early-stage assessments of data privacy queries by answering questions and suggesting when potential complaints should be lodged.[273]

In 2019 and 2020, respectively, Ireland's Department of Information and Assessment received 48,500 and 35,200 contacts related to data privacy: 22,300 and 23,200 emails, 22,200 and 10,000 phone calls, as well as 4,000 and 2,000 letters through post.[274] Ireland relies on the early-stage assessment tool as their DPA reportedly receives 150 and 144 new complaints every week in 2019 and 2020, respectively—with a growing number of data subjects finding "novel ways" to apply the GDPR, according to Data Protection Commissioner Helen Dixon.[275]

269. *See generally* GDPR, *supra* note 23, art. 58.

270. *See Overview on Resources*, *supra* note 249, at 10.

271. *See Complaints Handling—Data Protection Notice*, EUR. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/our-role-supervisor/complaints-handling-data-protection-notice_en [https://perma.cc/D4A5-H6YC].

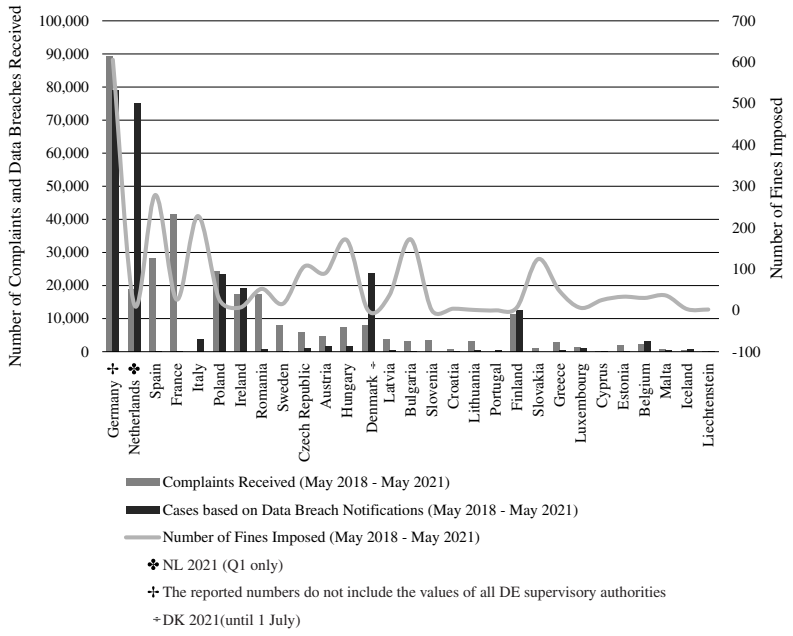
272. *See* INFO. COMM'R'S OFF., GDPR: ONE YEAR ON 4–6 (May 30, 2019), https://ico.org.uk/media/about-the-ico/documents/2614992/gdpr-one-year-on-20190530.pdf [https://perma.cc/NQ8L-UCG8].

273. *See* DATA PROT. COMM'N, ANNUAL REPORT 14–16 (2020) [hereinafter ANNUAL REPORT (2020)], https://www.dataprotection.ie/sites/default/files/uploads/2021-05/DPC%202020%20Annual%20Report%20%28English%29.pdf [https://perma.cc/WA3E-ELLU].

274. *Id.* at 15; DATA PROT. COMM'N, ANNUAL REPORT 14 (2019) [hereinafter ANNUAL REPORT (2019)], https://www.dataprotection.ie/sites/default/files/uploads/2020-04/DPC%20Annual%20Report%202019.pdf [https://perma.cc/BVE3-6BX4].

275. Simon Carswell, *Big Tech 'Procedural Queries' Delay Decision on First Data Fines—Watchdog,* IRISH TIMES (Feb. 20, 2020, 5:00 AM), https://www.irishtimes.com/business/technology/big-tech-procedural-queries-delay-decision-on-first-data-fines-watchdog-1.4178751 [https://perma.cc/35FK-W6KX].

FIGURE 19: DATA PRIVACY COMPLAINTS AND DATA BREACH NOTIFICATIONS RECEIVED VERSUS FINES IMPOSED IN THE E.U.[276]



Despite the large volume of complaints submitted, the number of fines issued in the first three years of the GDPR's operation has remained low. By October 8, 2021, E.U. nations (including the United Kingdom) had issued 809 fines under the GDPR, totaling over one billion euros. [277] Spain takes the quantitative lead, having imposed 301 fines to date since the GDPR's inception;[278] the Spanish DPA has received 18,480 complaints and 1,434 reports of data breaches since May 25, 2018.[279] Germany—despite having the largest DPA in terms of both budget and staff—has imposed just thirty-three fines, as of October 8, 2021.[280] Numerous supervisory authorities have attributed the disparity between the number of complaints received and fines issued to a lack of resources.[281]

Supervisory authorities have reported that the cooperation mechanism in which cross-border cases are compelled to operate creates significantly

276. *See Overview on Resources*, *supra* note 249, at 10, 15.
277. *Fines Statistics*, *supra* note 198.
278. *Id.*
279. EUR. DATA PROT. BD., EVALUATION OF THE GDPR UNDER ARTICLE 97—QUESTIONS TO DATA PROTECTION AUTHORITIES/EUROPEAN DATA PROTECTION BOARD: ANSWERS FROM THE SPANISH SUPERVISORY AUTHORITIES 12 (2020) [hereinafter ANSWERS FROM SPAIN], https://edpb.europa.eu/sites/default/files/es_sa_gdpr_art_97questionnaire.pdf [https://perma.cc/9TLH-Y4XP].
280. *Fines Statistics*, *supra* note 198.
281. *See id.*; *Individual Replies from the Data Protection Supervisory Authorities*, *supra* note 276.

longer investigations and decision-making proceedings.[282] Compulsory measures such as the exchange of relevant information and case development notifications often proceed at a slow pace.[283] 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.[284] As a result, expenditures on independent translation services are sometimes required.[285] 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 coordination across multiple member states.[286]

The novel and complex legal issues presented during GDPR investigations and proceedings require substantial expenditures on legal counsel.[287] When overseeing cross-border cases, the DPA must take into account the citizenship of the impacted data subject to ensure compliance with the national procedural rules of the member state.[288] Italy's DPA reported that the additional legal research and dialogue required between member states during cross-border proceedings has lengthened proceedings and delayed sanctions.[289] Germany, with a reported budget of €94,793,900 (more than double that of Italy's), has voiced similar complaints as its federal and state DPAs face a backlog totaling 19,752 cases, some extending as far back as 2017.[290]

---

282. Press Release, Hamburg Commissioner for Data Protection and Freedom of Information, Data Protection as Fundamental Right—Big Demand, Long Delivery Time (Feb. 13, 2020), https://datenschutz-hamburg.de/assets/pdf/2020-02-13_press-release_annual_report_2019.pdf [https://perma.cc/VHG5-QGDX].

283. *See, e.g.*, ANSWERS FROM SPAIN, *supra* note 279, at 10.

284. *See, e.g.*, EUR. DATA PROT. BD., EVALUATION OF THE GDPR UNDER ARTICLE 97—QUESTIONS TO DATA PROTECTION AUTHORITIES/EUROPEAN DATA PROTECTION BOARD: ANSWERS FROM THE FRENCH SUPERVISORY AUTHORITIES 7 (2020), https://edpb.europa.eu/sites/default/files/fr_sa_gdpr_art_97questionnaire.pdf [https://perma.cc/TY8E-5Q8V].

285. *See, e.g.*, *id.*

286. EUR. DATA PROT. BD., EVALUATION OF THE GDPR UNDER ARTICLE 97—QUESTIONS TO DATA PROTECTION AUTHORITIES/EUROPEAN DATA PROTECTION BOARD: ANSWERS FROM THE BULGARIAN SUPERVISORY AUTHORITIES 5 (2020), https://edpb.europa.eu/sites/default/files/bg_sa_gdpr_art_97questionnaire.pdf [https://perma.cc/L3QC-4U6L]; EUR. DATA PROT. BD., EVALUATION OF THE GDPR UNDER ARTICLE 97—QUESTIONS TO DATA PROTECTION AUTHORITIES/EUROPEAN DATA PROTECTION BOARD: ANSWERS FROM THE GERMAN SUPERVISORY AUTHORITIES 16 (2020) [hereinafter ANSWERS FROM GERMANY], https://edpb.europa.eu/sites/default/files/de_sas_gdpr_art_97questionnaire.pdf [https://perma.cc/LQ54-FAWU].

287. *See, e.g.*, ACCESS NOW, *supra* note 259 at 3 ("Fear of legal costs and delay tactics have sharply limited the capacity of DPAs to move forward key cases against tech giants whose revenues are sometimes higher than the DPAs' budgets.").

288. *See* ANNUAL REPORT (2019), *supra* note 274 at 9, 90.

289. EUR. DATA PROT. BD., EVALUATION OF THE GDPR UNDER ARTICLE 97—QUESTIONS TO DATA PROTECTION AUTHORITIES/EUROPEAN DATA PROTECTION BOARD: ANSWERS FROM THE ITALIAN SUPERVISORY AUTHORITIES 3 (2020), https://edpb.europa.eu/sites/default/files/it_sa_gdpr_art_97questionnaire.pdf [https://perma.cc/V356-7M92].

290. *See Overview on Resources*, *supra* note 249, at 11. The backlog of cases does not include the values of all DE authorities.

Individual cases can prove extremely costly for regulators. A single investigation into Cambridge Analytica carried out by the U.K data protection authority cost £2.4 million (about $3.1 million) and took more than three years.[291] The investigation required the DPA to review forty-two laptops and computers, 700 terabytes of data, thirty-one servers, over 300,000 documents, and a wide range of material in paper form and from cloud storage devices.[292] After the Austrian activist Max Schrems successfully obtained a decision from the Court of Justice of the European Union concerning cross-border data transfers to the United States,[293] Ireland was ordered to pay his legal costs—a bill estimated to exceed €2 million.[294]

On average, each of the eleven lawyers in the Austrian data protection authority simultaneously manages over one hundred cross-border and national cases.[295] 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.[296]

Procedural queries by the legal teams of investigated data controllers further delay the decision-making process.[297] The DPAs oversee the regulation of data processors with revenues that are grossly larger than their budget.[298] A notable example is Luxembourg, which allocates €5 million for data protection enforcement—to include enforcing data protection against companies such as Amazon.[299] But despite its small size, the DPA recently issued a $887 million fine against Amazon, which the company is

291. Izabella Kaminska, Opinion, *ICO's Final Report into Cambridge Analytica Invites Regulatory Questions*, FIN. TIMES (Oct. 8, 2020), https://ftalphaville.ft.com/2020/10/06/1602008755000/ICO-s-final-report-into-Cambridge-Analytica-invites-regulatory-questions [https://perma.cc/XLJ6-E7QP].

292. Natasha Lomas, *Cambridge Analytica Sought to Use Facebook Data to Predict Partisanship for Voter Targeting, UK Investigation Confirms*, TECHCRUNCH (Oct. 6, 2020), https://techcrunch.com/2020/10/06/cambridge-analytica-sought-to-use-facebook-data-to-predict-partisanship-for-voter-targeting-uk-investigation-confirms [https://perma.cc/C5KV-95GG].

293. Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (Schrems II), ECLI:EU:C:2020:559, ¶ 343 (July 16, 2020).

294. Cianan Brennan, *Data Protection Commission Hit with Massive Legal Bill After Facebook Privacy Case*, IRISH EXAM'R (Oct. 30, 2020), https://www.irishexaminer.com/news/arid-40073378.html [https://perma.cc/5645-WY3W].

295. EUR. DATA PROT. BD., EVALUATION OF THE GDPR UNDER ARTICLE 97—QUESTIONS TO DATA PROTECTION AUTHORITIES/EUROPEAN DATA PROTECTION BOARD: ANSWERS FROM THE AUSTRIAN SUPERVISORY AUTHORITIES 6 (2020), https://edpb.europa.eu/sites/default/files/at_sa_gdpr_art_97questionnaire.pdf [https://perma.cc/WV9R-EG27].

296. EUR. DATA PROT. BD., EVALUATION OF THE GDPR UNDER ARTICLE 97—QUESTIONS TO DATA PROTECTION AUTHORITIES/EUROPEAN DATA PROTECTION BOARD: ANSWERS FROM THE MALTESE SUPERVISORY AUTHORITIES 5 (2020), https://edpb.europa.eu/sites/default/files/mt_sa_gdpr_art_97questionnaire.pdf [https://perma.cc/QU66-X28Y].

297. ACCESS NOW, *supra* note 259, at 10.

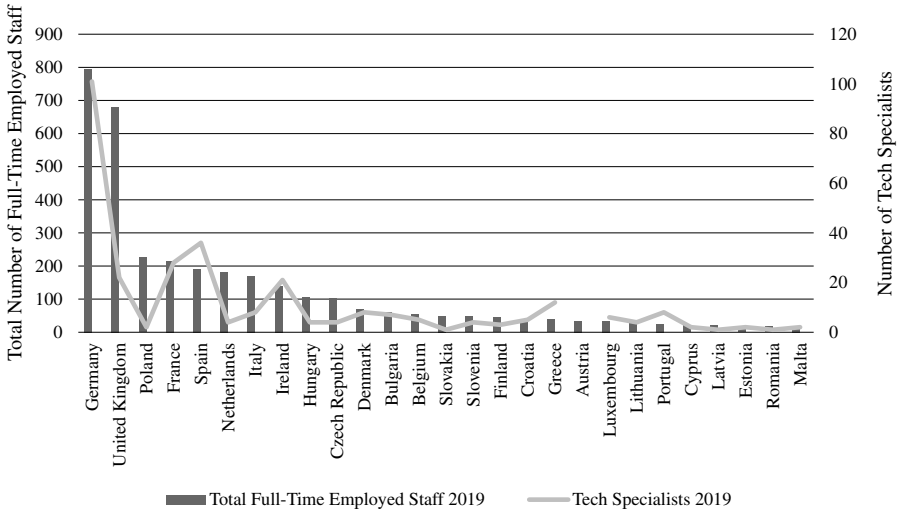
298. *See id.*

299. *Id.*

currently challenging.[300]

The GDPR also creates a private right of action for material or non-material damage suffered from a breach of data privacy laws.[301] Pursuant to article 78, a data subject may seek a judicial remedy before the courts of the supervisory authority's member state.[302] 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.[303] 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.[304] 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.[305]

FIGURE 20: 2019 DPA STAFF IN EUROPE: TOTAL STAFF VERSUS TECH SPECIALISTS[306]



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

300. Richard Lawler, *Amazon Fined Record $887 Million over EU Privacy Violations*, VERGE (July 30, 2021, 9:07 AM), https://www.theverge.com/2021/7/30/22601661/amazon-gdpr-fine-cnpd-marketplace-antitrust-data [https://perma.cc/T8RT-984V].

301. *See* GDPR, *supra* note 23, art. 78.

302. *Id.*

303. *Id.* arts. 77, 78(2).

304. *Id.* art. 80(1).

305. *See Fines Statistics*, *supra* note 198; RYAN & TONER, *supra* note 250, at 1.

306. RYAN & TONER, *supra* note 250, at 3–5, 7–8. The vacancies are included in the count and full-time equivalents are rounded. Data on Austria's tech specialists is unavailable.

DPAs employ five or fewer technology specialists.[307] 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.[308] Although Germany contributes 29% of Europe's technology specialists, the country has received similar complaints from state-level DPAs.[309] The recruitment and retainment of tech specialists has also proven challenging, particularly in DPAs with restrictive budgets.[310] Fourteen of these DPAs have annual budgets under €5 million, making it more difficult to ensure sufficient personnel to examine data practices.[311]

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.[312]

B. Enforcement in the United States

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, HIPAA is enforced principally by the Office for Civil Rights (OCR) of DHHS.[313] In the financial sector, the GLBA is enforced by several banking regulators, as well as the FTC.[314] Each of these regulators is funded separately by the U.S. federal government. The FTC also serves as a de facto privacy regulator under its responsibility to regulate unfair and deceptive practices.[315]

The following sections provide an overview of the U.S. data protection regulations at federal and state levels. They focus on the enforcement of

---

307. *Id.* at 7.

308. *See id.* at 3; Eur. Data Prot. Bd., Evaluation of the GDPR Under Article 97—Questions to Data Protection Authorities/European Data Protection Board: Answers from the Belgian Supervisory Authorities 3 (2020), https://edpb.europa.eu/sites/default/files/be_sa_gdpr_art_97questionnaire.pdf [https://perma.cc/YWR9-UX54]; Eur. Data Prot. Bd., Evaluation of the GDPR Under Article 97—Questions to Data Protection Authorities/European Data Protection Board: Answers from the Czech Supervisory Authorities 7 (2020), https://edpb.europa.eu/sites/default/files/cz_sa_gdpr_art_97questionnaire.pdf [https://perma.cc/5V52-L8MX].

309. *See* Ryan & Toner, *supra* note 250, at 4; Answers from Germany, *supra* note 286, at 5.

310. *See* Ryan & Toner, *supra* note 250, at 10.

311. *See id.* at 4–5.

312. Info. Comm'r's Off., *supra* note 272, at 18–19.

313. *HIPAA Enforcement*, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html#:~:text=HIPAA%20Enforcement,the%20Privacy%20and%20Security%20Rules [https://perma.cc/HVG8-TAR2].

314. Shelby Hiter, *GLBA Compliance & Standards*, Datamation (July 2, 2021), https://www.datamation.com/big-data/glba-compliance [https://perma.cc/74X5-HH84].

315. *See Privacy and Security Enforcement*, Fed. Trade Comm'n, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement [https://perma.cc/7D6J-LRS2] ("When companies tell consumers they will safeguard their personal information, the FTC can and does take law reinforcement action to make sure companies live up [to] these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them . . . .").

two major privacy laws—HIPAA and GLBA. Then, we turn to examine the cost of enforcement for the regulatory agencies.

1. HIPAA Enforcement Costs

The OCR of DHHS enforces the HIPAA Privacy, Security, and Breach Notification Rules.[316] The OCR also promotes broad awareness of HIPAA rights and protections.[317] It issues regulations and guidance, exacts civil monetary penalties, and pursues investigations and settlement agreements.[318] The OCR funds its HIPAA enforcement efforts through the civil monetary settlement funds it collects and discretionary budget allocations.[319]

FIGURE 21: HIPAA ENFORCEMENT BUDGET AND PERSONNEL—TABLE[320]

Fiscal Year	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
Discretionary Budget Authority	$39M	$39M	$39M	$39M	$30M	$30M
Civil Monetary Settlement Funds	$24M	$20M	$8M	$13M	$23M	$27M
Total	$63M	$59M	$47M	$52M	$53M	$57M
Number of Employees (Full-Time Equivalents)	170	179	138	155	159	156

316. U.S. DEP'T HEALTH & HUM. SERVS., PUTTING AMERICA'S HEALTH FIRST: FY 2020 PRESIDENT'S BUDGET FOR HHS 148 (2020) [hereinafter HHS BUDGET 2020].

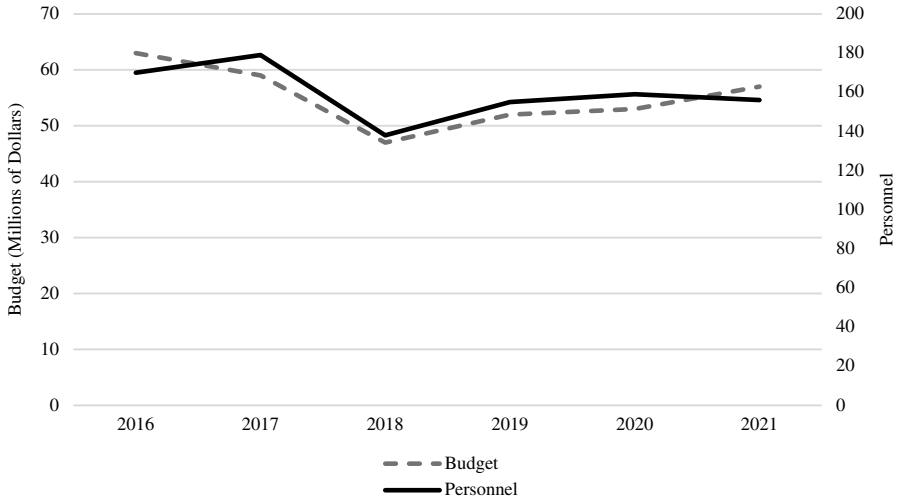
317. *Id.*

318. *Id.* at 147–48.

319. *See id.* at 147.

320. *Id.* at 147–48; U.S. DEP'T HEALTH & HUM. SERVS., PUTTING AMERICA'S HEALTH FIRST: FY 2021 PRESIDENT'S BUDGET FOR HHS 171–72 (2020) [hereinafter HHS BUDGET 2021]; U.S. DEP'T HEALTH & HUM. SERVS., PUTTING AMERICA'S HEALTH FIRST: FY 2019 PRESIDENT'S BUDGET FOR HHS 124–25 (2018) [hereinafter HHS BUDGET 2019]; U.S. DEP'T HEALTH & HUM. SERVS., PUTTING AMERICA'S HEALTH FIRST: FY 2018 PRESIDENT'S BUDGET FOR HHS 95–96 (2017) [hereinafter HHS BUDGET 2018].

FIGURE 22: HIPAA ENFORCEMENT BUDGET AND PERSONNEL—GRAPH[321]



From 2016 to 2019, the OCR's use of the Discretionary Budget remained consistent at $39 million but decreased to $30 million in 2020.[322] The shortfall was more than made up for, however, by increased amounts available for enforcement from the Civil Monetary Settlement Fund, which amounted to $8 million, $13 million, and $23 million in 2017, 2018, and 2019, respectively.[323] The number of employees, however, has decreased overall in recent years.[324]

2. FTC and Privacy and Data Security Enforcement

In addition to the broad power it holds under the FTCA, the FTC also enforces a variety of other statutes, including the GLBA, 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.[325] 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.[326]

321. HHS BUDGET 2021, *supra* note 320, at 171–72; HHS BUDGET 2020, *supra* note 316, at 147–48; HHS BUDGET 2019, *supra* note 320, at 124–25, HHS BUDGET 2018, *supra* note 320, at 95–96.

322. *See supra* Figure 21.

323. *Id.*

324. *See supra* Figure 22.

325. FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE 1 (2019).

326. *Id.* at 2, 15.

While the FTC's overall enacted budget in fiscal year 2019 was $309.7 million with 1,130 full-time employees, its budget and staff for privacy enforcement represents a small share of these larger totals.[327] Despite an increase in workload, the FTC's budget for privacy enforcement remained remarkably stagnant until 2020, a year in which it also undertook a record number of enforcement actions.[328] The FTC raised its privacy enforcement budget for 2021 to almost $13 million.[329] The amounts still seem grossly insufficient to undertake the enormous task of privacy enforcement across a nation the size of the United States.[330]

FIGURE 23: FTC SPENDING AND WORKFORCE DEDICATED TO PRIVACY ENFORCEMENT[331]

Fiscal Year	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
Privacy and Identity Protection	$10M	$10.1M	$9.9M	$9.9M	$12.6M	$12.8M
Number of Employees (Full-Time Equivalents)	57	54	52	52	61	61

327. *See* FED. TRADE COMM'N, FISCAL YEAR 2021 CONGRESSIONAL BUDGET JUSTIFICATION 46 (2020) [hereinafter FTC FISCAL YEAR 2021 BUDGET JUSTIFICATION]

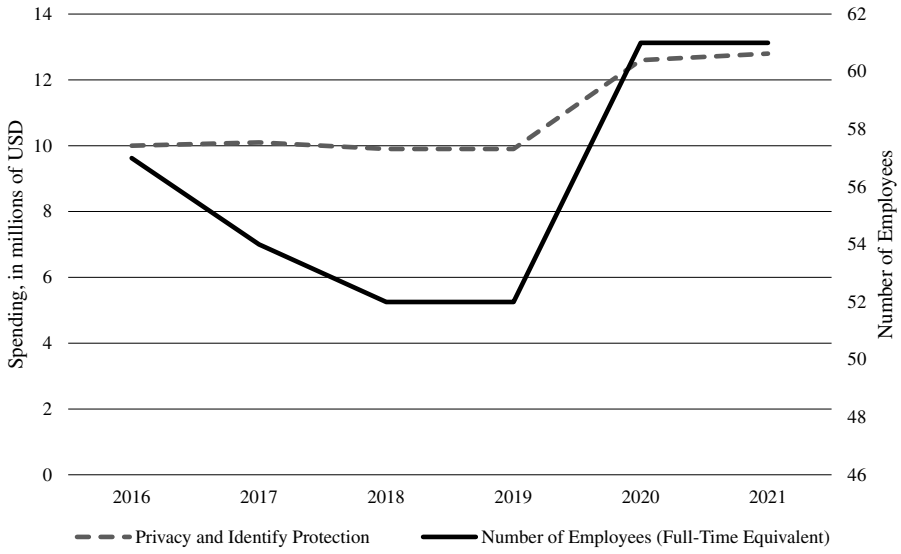
328. *See id.* at 5–16.

329. *Id.* at 121.

330. *See generally* Lindsey Barrett, Laura Moy, Paul Ohm & Ashkan Soltani, *Illusory Conflicts: Post-Employment Clearance Procedures and the FTC's Technological Expertise*, 35 BERKELEY TECH. L.J. 793 (2021).

331. FTC FISCAL YEAR 2021 BUDGET JUSTIFICATION, *supra* note 327, at 121; U.S. FED. TRADE COMM'N, FISCAL YEAR 2018 CONGRESSIONAL BUDGET JUSTIFICATION 141 (2017) [hereinafter FTC FISCAL YEAR 2018 BUDGET JUSTIFICATION]; FED. TRADE COMM'N, FISCAL YEAR 2017 CONGRESSIONAL BUDGET JUSTIFICATION 131 (2016) [hereinafter FTC FISCAL YEAR 2017 BUDGET JUSTIFICATION].

FIGURE 24: FTC PRIVACY PROTECTION: EXPENDITURES AND NUMBER OF EMPLOYEES[332]



3. California Consumer Privacy Act

The California Department of Justice enforces privacy laws through its Consumer Law Unit and its Privacy Unit.[333] Even prior to the passage of the CCPA, California had enforced various data protection laws including the Data Breach Notification Statute.[334] With the coming of the CCPA, the California Department of Justice has requested an additional twenty-three full-time employees at an estimated cost of approximately $4.5 million per year.[335]

C. ENFORCEMENT IN CHINA

Multiple agencies enforce Chinese privacy and cybersecurity law. While China does not have any single "supervisory authority dedicated to

332. FTC FISCAL YEAR 2021 BUDGET JUSTIFICATION, *supra* note 327, at 121; FTC FISCAL YEAR 2018 BUDGET JUSTIFICATION, *supra* note 331, at 141; FTC FISCAL YEAR 2017 BUDGET JUSTIFICATION, *supra* note 331, at 131.

333. *California Attorney General Creates Privacy Enforcement and Protection Unit*, WINSTON & STRAWN: PRIVACY & DATA SEC. L. BLOG (July 26, 2012), https://www.winston.com/en/privacy-law-corner/california-attorney-general-creates-privacy-enforcement-and-protection-unit.html [https://perma.cc/9D25-8FFV].

334. CAL. CIV. CODE §§ 1798.25–1798.78 (requiring a business or a government agency that owns or licenses unencrypted computerized data that includes personal information, as defined, to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person).

335. Amy C. Pimentel, *Little by Little, Attorney General Becerra Sheds Light on the CCPA in 2020*, MCDERMOTT WILL & EMERY (Jan. 8, 2020), https://www.mwe.com/insights/little-by-little-attorney-general-becerra-sheds-light-on-the-ccpa-in-2020 [https://perma.cc/L92M-QS3L].

the protection of personal information,"[336] the Cyberspace Administration of China is generally considered the primary data protection authority in China.[337] 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.[338] Enforcement can also occur at the provincial level.[339] 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."[340]

In recent years, the Chinese government has launched campaigns against the misuse of information by mobile apps.[341] 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.[342] The following table outlines the work of their campaigns.

FIGURE 25: MIIT, MPS, AND SAMR ENFORCEMENT CAMPAIGNS[343]

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 100+ companies to rectify their policies on the collection and use of personal data	Requested twenty-seven companies to rectify problems; issued warnings against sixty-three companies; fined ten companies; commenced criminal investigations into two companies	Investigated 1,474 cases of consumer information infringement; fined 19.64+ million yuan

While there is no overall estimate of the amount China's public sector spends to enforce its Cybersecurity Law and 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.

336. Pernot-Leplay, *supra* note 61, at 86.
337. DLA PIPER, *supra* note 223, at 158.
338. *Id.*
339. *See id.*
340. *Id.*
341. *Id.* at 164.
342. DAI & DENG, *supra* note 98, at 16–17.
343. *Id.*

FIGURE 26: EXPENDITURES OF LOCAL CYBERSPACE ADMINISTRATION BRANCHES

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

V. CONCLUSION

Getting data privacy law right is critical for every country in the twenty-first century. The digital economy depends on a proper legal framework that protects privacy. Our study shows that even the expenditures from the United States and the European Union are not out of reach for 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 can still take steps, such as relaxed mandates for small- and medium-sized businesses or ex post facto liability rules for negligent or intentional abuses 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. Though the costs of compliance may seem high, the costs of *not* having data privacy protection can be quite high as well; a lack of protection could cause consumers and other counterparties to avoid 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.[344]

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 should make it clear what companies can do to reduce costs and increase compliance. Experts we spoke with commonly complained that it can be difficult to know how to comply with both E.U. and Chinese data privacy law. The GDPR's complex framework (there are 173 recitals, ninety-nine articles, and multiple guidance

344. *See generally* WORLD BANK GRP., WORLD DEVELOPMENT REPORT 2020: TRADING FOR DEVELOPMENT IN THE AGE OF GLOBAL VALUE CHAINS (2020).

documents) generally requires expensive legal counsel to navigate.[345] One interviewee noted that a hospital participating in a clinical research trial with a drug company might be classified as a processor, joint controller, or controller in its own right, depending on which authority is interpreting the rules. A recent case from the Court of Justice of the European Union requires companies to hire lawyers to give opinions on foreign intelligence laws of every country to which the companies are transferring information outside of the European Union.[346] For these companies, the Chinese rules may be highly detailed, but that detail often exists 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 cost of data localization. Data localization is a particularly expensive and burdensome mandate. Rather than hosting their own servers or managing their own cybersecurity, businesses increasingly depend on cloud service providers. Data localization imposes additional costs on local micro, small, and medium enterprises (MSMEs), 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 bear the expense or 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 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 that operates in multiple jurisdictions to follow similar 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 E.U.–U.S. Privacy Shield, or the CCPA automatically is also compliant with that national privacy law. This would have the added benefit of encouraging global companies to offer services in that jurisdiction.

Consider burdens on small enterprises. Regulatory complexity poses a special challenge for MSMEs that do not have the resources to hire lawyers to create tailored privacy programs; rework their information technology to allow for the realization of rights to access, correct, and delete

345. DATAGRAIL, *supra* note 126, 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).

346. Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (Schrems II), ECLI:EU:C:2020:559, ¶ 343 (July 16, 2020).

information; and hire information security providers to protect data. 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 personal information about others, whether a friend or a business counterparty, on their phone). One expert in Brazil noted that under the current law, even the local baker might have to appoint a data protection officer, at least until a federal regulator issues exemption for such businesses. One response to this problem is to provide exceptions for smaller enterprises from certain requirements. For example, the CCPA 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.[347] By contrast, the Nigerian Data Privacy Regulation sets a much lower threshold, requiring data controllers who process the personal data of more than 2,000 subjects in a year to performs audits.[348]

Establish models conducive to cross-border data transfers. Many countries have modeled their laws after 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 E.U. residents, making it easier to supply services to the large E.U. 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 favorable adequacy decisions from the European Union.[349] Furthermore, the standard for receiving a favorable adequacy decision only appears to have become stricter over time. Japan was recently recognized with an adequacy decision, but only after "80 rounds of negotiations played out over 300 hours" taking place between April 2016 and January 2019.[350] Only one country is currently being considered for an adequacy decision: South Korea.[351] 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

347. This latter figure is scheduled to go up to 100,000 when the California Privacy Rights Act goes into effect.

348. *Nigeria Issues New Data Protection Regulation*, HUNTON ANDREWS KURTH: PRIV. & INFO. SEC. L. BLOG (Apr. 5, 2019), https://www.huntonprivacyblog.com/2019/04/05/nigeria-issues-new-data-protection-regulation [https://perma.cc/VX3X-Q5GD].

349. Robert Carolina, *Why the EU Has Issued Relatively Few Data Protection Adequacy Determinations? A Reply*, LAWFARE (Jan. 13, 2017, 12:52 PM), https://www.lawfareblog.com/why-eu-has-issued-relatively-few-data-protection-adequacy-determinations-reply [https://perma.cc/3WV3-PR73] (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").

350. 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 [https://perma.cc/Z867-EGYD].

351. *See* Joint Statement by Commissioner Reynders and Yoon Jong In, Chairperson of the Personal Information Protection Commission of the Republic of Korea, EUROPEAN COMM'N (Mar. 30, 2021), https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1506 [https://perma.cc/AQZ8-DYKV].

personal data, from Standard Contractual Clauses and Binding Corporate Rules to newer possibilities for certifications and codes of conduct.[352] 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 E.U.–U.S. 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 E.U.–U.S. Privacy Shield on the grounds that it did not provide sufficient legal rights to European residents to challenge U.S. foreign surveillance.[353] 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,[354] it represents a workable attempt to meet core E.U. concerns with data privacy in a way that companies seem to manage; its principles could 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 the 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 data; and (7) provide recourse for complaints.[355] In addition, companies must abide by sixteen supplementary principles.[356]

***

The study also reveals the need for further inquiry. Private companies are reluctant to publish information about the costs of compliance, which

352. *See* GDPR, *supra* note 23, arts. 44–49. Our survey respondents indicated that they rely principally on standard contractual clauses for cross-border data transfer from the European Union.

353. *See* Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 J. INT'L ECON. L. 771, 774 (2020).

354. WORLD BANK GRP., *supra* note 344, at 245 ("The EU-U.S. Privacy Shield offers a way of resolving the conflict between regulatory heterogeneity and international data flows.")

355. *See Privacy Shield Overview*, PRIV. SHIELD FRAMEWORK, https://www.privacyshield.gov/program-overview [https://perma.cc/Q5MY-XLRQ].

356. *See id.*

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.