Indiana Journal of Global Legal Studies

Indiana Journal of Global Legal Studies

Volume 28 | Issue 2 Article 7

Summer 8-1-2021

# How the World's Largest Economies Regulate Data Privacy: Drawbacks, Benefits, & Proposed Solutions

Alexander J. Pantos
*Indiana University Maurer School of Law*, apantos@iu.edu

# How the World's Largest Economies Regulate Data Privacy: Drawbacks, Benefits, & Proposed Solutions

ALEXANDER J. PANTOS*

## INTRODUCTION

National data privacy regimes are quickly gaining traction and ubiquity around the globe. Moving forward, countries will face a range of difficult decisions surrounding how best to engage internationally in cross border data flow, particularly in the context of personal information (PI).

This article takes a bird's-eye view of the current state of data privacy regimes in the world's four highest GDP regions. In part, this article hopes to provide a succinct analysis of these data privacy regimes, with a focus on the balance they strike between granting individuals rights in their data and placing responsibilities on businesses that deal with PI. Analyzing the world's most economically active countries provides an opportunity to highlight the substantial benefits that data privacy regimes can provide the world's citizens while balancing these benefits against the potential negative economic impact of data privacy regimes. This proposition motivated this article's choice of regions to survey.

Section I provides an overview of the current state of data privacy legislation and regulation in the United States, China, Japan, and the European Union. Section II outlines the drawbacks to some of the common themes that emerge from these surprisingly similar regulatory frameworks. Section III explores the benefits data privacy regimes offer to individuals. Section IV proposes potential solutions to this emerging global governance conundrum.

---

* J.D. Candidate, Indiana University Maurer School of Law, 2021. I would like to thank Professor Michael Mattioli for his guidance in writing this article; the Indiana Journal of Global Legal Studies team for their support and editorial work; and Alexa Wilson for her patience, advice, and willingness to look over the drafts that lead to this piece. Any remaining errors are my own.

Indiana Journal of Global Legal Studies Vol. 28 #2 (Spring 2021)

## I. SURVEY OF SELECT CURRENT GLOBAL DATA PRIVACY REGIMES

This section focuses on major national players in the global data privacy scheme, specifically those countries with the world's four largest GDPs,[1] whose data privacy regimes vary in important ways.

### *United States*

The United States federalist system of government creates unique challenges in data privacy regulation. This subsection outlines privacy laws at the federal level and in California to highlight the relevant features of each and illustrate the complex, interconnected nature of United States data privacy governance.

#### *Federal Privacy Law Patchwork*

The United States (US) does not have a comprehensive federal framework for private data governance.[2] The closest approximation at the federal level is a variety of modality-focused, content-focused, and child-safety-focused laws passed throughout the late twentieth and early twenty-first centuries.[3]

Modality-focused laws limit the way commercial entities can contact consumers using specific modes of communication.[4] For example, the Telephone Consumer Protection Act (TCPA) proscribes commercial autodialing of any emergency numbers, guest rooms at facilities with sensitive clientele like retirement homes and hospitals, and cellular phones.[5] The Controlling the Attack of Non-Solicited Pornography and Marketing Act (CAN-SPAM) focuses instead on the notorious spam email and sets guidelines for companies using email to communicate with private individuals.[6] The congressional findings in CAN-SPAM focus on the efficiency-draining effects spam email has on commerce and the potential for spam emails to contain "vulgar or pornographic" content that may be offensive to some email users.[7] Section 7704 of CAN-SPAM provides, in part, that commercial mass-mailers may not

---

1. *GDP (Current US$)*, THE WORLD BANK, https://data.worldbank.org/indicator/ny.gdp.mktp.cd?most_recent_value_desc=true (Last Visited Oct. 9, 2019).
2. *See* Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States?*, 23 J. TECH L. & POL'Y 68, 73-74 (2018).
3. *Id.* at 73-84.
4. *Id.* at 74.
5. *Id.*
6. *Id.*
7. 15 U.S.C.A. § 7701(a)(2), (5) (West 2019).

use false or misleading information in subject lines,[8] and must include mechanisms for email recipients to opt out of future emails.[9] Section 7703 imposes criminal punishment for violations by identifying CAN-SPAM as an addition to a statute criminalizing fraud and related activity in email communications.[10]

Content-focused privacy laws "seek to regulate privacy in the context of specific types of data or industries."[11] The Health Insurance Portability and Accountability Act (HIPAA) protects individuals' health information by establishing national standards for privacy and security measures for "covered entities"[12] that hold and transfer health data.[13] In light of the strong public policy interests in favor of facilitating the transfer of such data between medical care and research institutions,[14] HIPAA also standardizes the format covered entities use to store health information to make transfers more efficient.[15] The Fair Credit Reporting Act (FCRA) and its subsequent amendments (namely, the Consumer Credit Reporting Reform Act of 1996 and the Fair and Accurate Credit Transactions Act of 2003)[16] "promote[] the accuracy, fairness, and privacy of information in the files of consumer reporting agencies."[17] In response to the often opaque practices of consumer reporting agencies,[18] the FCRA focuses on consumers' rights in relation to the information agencies hold about them, including the right to be told if your information has been used against you, the right to know what is in your credit file, and the right to dispute inaccurate or incomplete information.[19]

---

8. *Id.* § 7704(a)(2).

9. *Id.* § 7704(a)(3)-(4).

10. *Id.* § 7703(b)(1); *see generally* 18 U.S.C.A. § 1037 (West 2019) (authorizing punishment in the form of fines, prison time, and civil forfeiture for violation of the act).

11. Pardau, *supra* note 2, at 79.

12. MEDPRIVACY, GUIDE TO MEDICAL PRIVACY AND HIPAA § 200 (Joan M. Flynn ed.) (2015), 2002 WL 33833724 ("[A]ny health plan, health care provider or clearinghouse that electronically transmits or stores personal health information, including entities' business associates.").

13. *Id.*

14. *See* Michael Mattioli, *The Data-Pooling Problem*, 1 BERKELEY TECH. L.J. 179, 179-82 (2017) (exploring the use and transfer of big data in the context of cancer research).

15. MEDPRIVACY, *supra* note 12.

16. Pardau, *supra* note 2, at 79.

17. FED. TRADE COMM'N, A SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT, https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

18. *See generally* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014) (advocating for increased procedural due process in disputes between consumers and credit reporting agencies).

19. MEDPRIVACY, *supra* note 12.

The realm of child-safety-focused federal laws is dominated by the Children's Online Privacy Protection Act (COPPA).[20] COPPA requires verifiable parental consent before online data collectors can collect, use, or distribute children's information.[21] Passed in 1998, COPPA aims to protect society's most vulnerable, and often most gullible, citizens by imposing criminal penalties on website owners who do not comply.[22]

Their narrow scope is the greatest strength and greatest weakness of modality-, content-, and child-safety-focused laws. These laws regulate their respective areas of impact with specificity and efficacy but leave consumers' information open to misuse in areas that fall outside their reach. Notably, of the US federal laws discussed in this note, only COPPA covers data contained within or obtained from social media platforms and online search engines, which are arguably the most notorious data repositories for modern internet users. This lack of nationwide regulation could be chalked up to the slow-moving nature of the federal legislature. It also may be, however, that the federal government is counting on the US's federalist structure to shore up any leaks in the protection of citizens' privacy rights by assuming that states will enact such laws themselves. Such laws could account for the specific challenges each state's citizens face with respect to data privacy and could more accurately reflect each state's citizens' local values surrounding the collection and use of their data.

*California*

A notable example of this proposition is the state of California's Consumer Privacy Act (CCPA), which went into effect in 2020 and closely mirrors the European Union's General Data Protection Regulation (GDPR). The CCPA aims to give California's citizens more control over the personal data that businesses collect about them.[23] While the CCPA limits its reach to large businesses[24] that collect and

20. Pardau, *supra* note 2, at 82.
21. *Id.*
22. *Id.*
23. *See generally* Cal. Civ. Code § 1798.105 (West 2018).
24. Cal. Civ. Code § 1798.140(c) (West 2018) defines "business" as "[a] [company] . . . that collects consumers' private information, . . . determines the purpose and means of the processing of consumers' personal information, [and] that does business in the State of California . . . ." To fall under the regulation's purview, the businesses also must either have income of $25,000,000 annually; receive information from at least 50,000 consumers, households or devices; or derive 50% or more of its annual revenue from selling consumers' data. *Id.*

deal in PI,[25] it is still far broader and more comprehensive than the US piecemeal federal privacy regulations.[26]

The CCPA categorizes businesses as either data collectors or data sellers and establishes citizens' rights and businesses' responsibilities for each category.[27] In either context, consumers are granted the right to request that companies delete their personal data, and businesses are required to delete—and instruct service providers to delete—the data upon receipt of a "verifiable consumer request."[28]

Consumers have the right to direct businesses that sell data not to sell their PI; this is known in the CCPA as "the right to opt-out."[29] Businesses that sell data have concurrent responsibilities to disclose to consumers the fact that PI may be sold and inform consumers of their right to opt out of having their PI sold.[30] Additionally, these businesses must provide a link on their websites labeled "Do Not Sell My Personal Information" that provides a mechanism for consumers to opt out,[31] and they cannot sell PI if they have received direction from the consumer not to.[32] Citizens have the right to request disclosure of a wide range of information from businesses that sell their PI, including the categories of PI collected and sold.[33] Businesses that sell data have the responsibility to provide these disclosures free of charge within forty-five days of receipt of a verified consumer request.[34]

For data collection, consumers have a similar right to opt out, and businesses have the responsibility to provide, at a minimum, a toll-free telephone number and website address where consumers can exercise this right.[35] Similar to businesses that sell data, businesses that collect data have a responsibility to disclose information to consumers within forty-five days of receipt of a verified consumer request, including: the categories of information the business collects, to whom the business communicates the information, and the business purpose of the data collection.[36]

---

25. *Id.* at § 1798.140(o)(1) (PI "means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.").
26. *See* Pardau, *supra* note 2, at 89.
27. *See generally* Cal. Civ. Code. §§ 1798.100-.125 (West 2018).
28. *Id.* at § 1798.105(a), (c).
29. *Id.* at § 1798.120(a).
30. *Id.* at § 1798.120(b).
31. *Id.* at § 1798.135(a)(1).
32. *Id.* at § 1798.120(d).
33. *Id.* at § 1798.115(a).
34. *Id.* at § 1798.130(a)(2).
35. *Id.* at § 1798.130(a)(1).
36. *Id.* at § 1798.110(c).

Mirroring the federal government's COPPA, the CCPA provides special protection for children. Businesses are not allowed to sell data collected from children under thirteen-years-old without an express "opt in" from a parent or guardian.[37] For children thirteen-to-sixteen-years-old, parent or guardian consent is not required, but an opt in must be obtained from the children themselves.[38] While this may seem like a small difference, businesses that must follow an opt-in, rather than an opt-out, procedure are highly limited in their freedom to use information collected from California's children.

Finally, the CCPA goes to great lengths not to step on the toes of the federal government's existing privacy regimes.[39] Specifically, in cases of overlap with data covered by HIPPA and the FCRA, discussed above, the CCPA explicitly does not apply.[40] This careful tailoring lends credence to the argument that the federal government is planning its own privacy regulations around the assumption that states will pick up where the federal regulations leave off. As noted above, federal statutes do not cover information collected by social media websites and search engines. California, partially through its citizen ballot initiative procedure,[41] looked to the values of its citizens to fill the gaps left by the federal government. While not every state gives its citizens as much say in legislative procedure, it stands to reason that other states, faced with an increased focus on data collection and privacy concerns, will follow suit.[42]

*China*

In 2016, Xu Yuyu, a Chinese high school graduate preparing for college, was swindled into giving around $1,400 to a scammer posing as an education official.[43] Two days later, Yuyu died from cardiac arrest, which in the public's mind was tied to the anxiety she suffered following the scammer's attack.[44] This event, coupled with a number of other

37. *Id.* at § 1798.120(c).
38. *Id.*
39. *See* Pardau, *supra* note 2, at 93.
40. *Id.*
41. *Id.* at 90-91.
42. *See generally* Forbes Tech. Council, *How Will California's Consumer Privacy Law Impact the Data Privacy Landscape?*, FORBES, https://www.forbes.com/sites/forbestechcouncil/2018/08/20/how-will-californias-consumer-privacy-law-impact-the-data-privacy-landscape/#4e656637e922 (2018).
43. Wei Sheng, *One Year After GDPR, China Strengthens Personal Data Regulations, Welcoming Dedicated Law*, TECHNODE (June 19, 2019), https://technode.com/2019/06/19/china-data-protections-law/ (2019).
44. *Id.*

highly publicized data breaches, sparked national outrage over China's lack of data privacy regulation.[45] The Chinese government responded in the same year with the passage of the Cybersecurity Law (the Law).[46] Article 1 of the Law lays out its broad public policy goals; namely, to "safeguard cyberspace sovereignty and national security, . . . protect the lawful rights and interests of citizens, . . . and promote the healthy development of the informatization of the economy and society."[47]

Historically, China has relied on its "Great Firewall" to control what can and cannot be reached by end users within its borders.[48] The Chinese government is aided in this process by its exclusive control over Internet access providers (IAPs), all of which are connected to a "foreign Internet backbone."[49] China's Internet infrastructure allows the government to filter what information makes its way to end users based on whitelists (websites that are expressly allowed), blacklists (websites that are expressly disallowed), and keyword restrictions.[50]

While the Great Firewall protects information coming to end users, the Law looks to protect information collected from end users. The Law applies to "network operators and businesses in critical sectors."[51] "Network operators" is a broad term under the Law, which applies to network managers and owners of any group of computers or computer systems that gather, transmit, and process data.[52] "Critical sectors" is similarly broad, encompassing "communications, information services, energy, transport, water, financial services, public services, and electronic government services."[53]

Putting these broad definitions to work, Article 37 of the Law provides that network operators must store any PI collected in China within the country's borders and must ask for permission before any data is transferred out of the country.[54] The petitioning network

---

45. *Id.*

46. *Id.*

47. Rogier Creemers et al., *Translation: The Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, NEW AMERICA: CYBERSECURITY INITIATIVE (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

48. *See* Jyh-An Lee & Ching-Yi Liu, *Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China*, 13 MINN. J.L., SCI., & TECH. 129-34 (2012).

49. *Id.* at 133-34.

50. *See id.* at 131.

51. Jack Wagner, *China's Cybersecurity Law: What You Need to Know*, THE DIPLOMAT (June 01, 2017), https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

52. *Id.*

53. *Id.*

54. Creemers et al., *supra* note 47.

operator must show that the transfer is "truly necessary" and must allow a number of Chinese state entities to perform a "security assessment" to ensure proper cybersecurity measures are in place before the operator can transmit the PI across the Chinese border.[55]

The Law, by itself, is primarily an instrument to set out policy goals and broad privacy requirements.[56] To supplement the Law, China's National Information Security Standardization Technical Committee published TC260, or the Personal Information Security Specification (the Standard), "which covers the collection, storage, use, sharing, transfer, and disclosure of personal information."[57] The Standard covers a lot of ground and, like the CCPA, provides private individuals with a wide range of rights, and businesses with a wide range of responsibilities.[58] Thematically, the Standard can be broken down into three main categories: (1) requirements for explicit consent from data-collection subjects, (2) requirements for disclosing what the Standard refers to as "PI Controllers,"[59] and (3) requirements for privacy security infrastructure and personnel.[60]

The Standard's explicit consent requirement begins at collection and mandates that PI controllers must acquire separate consent each time they use the individual's PI after collection.[61] To illustrate, imagine a Chinese company uses PI to create materials that advertisers can use to supplement targeted advertising. At the point of collection, the company must obtain explicit consent from the data subject. If the company decides to share the data with an ad agency, the company must obtain the subject's separate, explicit consent. Down the road, if the company decides to use PI to create a new algorithm to provide feedback to their advertiser clients on the impacts of their advertisements, the company must obtain the subject's separate consent.

At each step in the consent process, PI controllers must provide a range of information about the natures and purposes of their data collection and retention.[62] For example, when collecting PI, the PI controller must disclose to the individual "the respective types of the PI

---

55. *Id.*

56. Sheng, *supra* note 43.

57. *Id.*

58. *See generally* Mingli Shi et al., *Translation: China's Personal Information Security Specification*, NEW AMERICA: CYBERSECURITY INITIATIVE (Feb. 8, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/.

59. *Id.* art. 3.4("An organization or individual that has the authority to determine the purposes and/or methods of the processing of PI").

60. *See generally id.*

61. *Id. art. 5.3.*

62. *See generally id.*

collected[;] . . . the rules of collecting and using the PI (e.g. purpose of collection and use; manner and frequency of collection; storage location; storage period; [the controller's] data security capabilities; information related to sharing, transferring, and public disclosure; etc.)."[63] The PI controller may only obtain express consent after disclosing this information to the individual.[64]

The Standard's infrastructure requirements include numerous triggers for performing Personal Information Security Impact Assessments[65] and provisions that require certain PI controllers operating in China to appoint a PI protection officer and create a PI protection division.[66] The PI protection officer and division are necessary if the PI controller's "main business involves the processing of PI and the number of employees exceeds 200" or "[the PI controller] [p]rocesses PI of more than 500,000 people or expects to process PI of more than 500,000 people within 12 months."[67] The Standard requires assessments when any new law or regulation is passed that bears on the PI controller's activities; when the PI controller's "business model, information system, or operational environment" changes; and in the event of any "major" security breaches.[68]

*Japan*

Japan recently espoused the principle of "Data Free Flow with Trust."[69] Shinzo Abe, Japan's prime minister, gave a speech at the World Economic Forum's annual meeting in early 2019 highlighting his vision for discussions of data-based governance at the June 2019 G20 summit.[70] The prime minister emphasized the ever-increasing importance of data in the global economy and called for international agreement and data governance based on protections for privacy data

63. *Id.* art. 5.3.

64. *Id.*

65. *Id.* art. 3.8: ("A process to evaluate: the degree to which PI processing complies with laws and regulations; whether there are any risks of damaging the lawful rights and interests of PI subjects; and how effective various measures are to protect PI subjects.").

66. *Id.* art. 7.1(d).

67. *Id.* art. 10.1(c).

68. *Id.* art. 10.2(c).

69. *See* NIGEL CORY ET AL., PRINCIPLES AND POLICIES FOR "DATA FREE FLOW WITH TRUST" 2 (Info. Tech. & Innovation Found. ed., 2019), https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust.

70. Shinzo Abe, *'Defeatism About Japan is Now Defeated': Read Abe's Davos Speech in Full*, WORLD ECON. FORUM (Jan. 23, 2019), https://www.weforum.org/agenda/2019/01/abe-speech-transcript/.

and the free flow of anonymous, societally-useful data to fuel innovation.[71]

Japan's Act on the Protection of Personal Information (APPI) currently controls the country's data privacy laws.[72] The APPI's purpose mirrors Prime Minister Abe's policy goals, explicitly balancing the goal of "protect[ing] an individual's rights and interests [in their PI]" with "the utility of personal information including that the proper and effective application of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched quality of life for the people of Japan."[73]

Similar to China's Standard, the APPI mandates that a "personal information handling business operator"[74] must specify and disclose a "utilization purpose"—in other words, what it uses an individual's PI for—when handling PI.[75] Consent must be acquired pre-collection if the operator is collecting "special care-required"[76] personal information.[77] In changing the utilization purpose, the operator must take care not to alter the purpose so much that it falls outside of the utilization purpose stated before consent was obtained,[78] and must obtain consent again if the new purpose falls outside of the original scope of consent given.[79]

As with California's CCPA and China's Law and Standard, the APPI applies to business operators that handle the data of individuals in Japan regardless of whether the business has a physical presence in Japan.[80] However, unlike the CCPA and the Standard, the APPI does not include any restrictions based on the size of the business or the amount of personal data collected.[81] When operators want to transfer

71. *Id.*

72. Andrada Coos, *Data Protection in Japan: All You Need to Know About APPI*, ENDPOINT PROTECTOR (Feb. 1, 2019), https://www.endpointprotector.com/blog/data-protection-in-japan-appi/.

73. Kojin jōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information (APPI)], Law No. 51 of 2016, art. 1 (Japan), translated by Pers. Info. Prot. Comm'n (2016).

74. *Id.* art. 2(5) ("a person providing a personal information database etc. for use in business").

75. *Id.* art. 15(1).

76. *Id.* art. 2(3) ("personal information comprising a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal.").

77. *Id.* at art. 17(2).

78. *Id.* art. 15(2).

79. *Id.* art. 16(2).

80. Coos, *supra* note 72.

81. *Id.*

data to a third party located within Japan's borders, they must obtain separate consent from the data subject for the transfer.[82] When operators want to transfer data to third parties located outside Japan's borders, the operator must ensure that the third party has "a personal information protection system recognized to have equivalent standards to that in Japan . . . ."[83] This requirement likely has a twofold purpose. First, on its face, the provision aims to protect Japanese citizens' PI after it leaves the hands of Japanese operators. However, less obviously, Japan likely intends this provision to act as an incentive to foreign countries and encourage them to follow its own footsteps by enacting similar laws and regulations around PI protection. Again, this mirrors Prime Minister Abe's goal of "Data Free Flow with Trust."

For data subjects, the APPI creates a number of rights concerning personal data. For example, a data subject can request that an operator disclose any personal data it has retained about the subject.[84] Upon review, a data subject can demand corrections for any information the operator holds that the subject determines is inaccurate,[85] withdraw consent for the retention of personal data at any time, and demand deletion.[86] If the operator does not meet any of these demands within a two-week window, the APPI creates a cause of action that allows data subjects to bring suit against offending operators.[87]

*European Union*

The EU's new General Data Protection Regulation (GDPR), which went into effect on May 25, 2018, has prompted a wide range of praise, criticism, and analysis. The stated purpose of the GDPR is to "protect[] . . . fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."[88] The GDPR has a wide scope and applies to broadly-defined "personal data"[89] that is processed by controllers relating to offering goods and services to—or monitoring the behavior of—EU citizens.[90] The GDPR, like California's CCPA,

82. APPI, art. 23(1).
83. *Id.* art. 24.
84. *Id.* at art. 28(1).
85. *Id.* at art. 29(1).
86. *See id.* art. 30(1).
87. *Id.* art. 34(1).
88. 2016 O.J. (L 119) 32.
89. *Id.* at 33 ("[A]ny information relating to an identified or identifiable natural person . . . such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.").
90. *Id.*

China's Law and Standard, and Japan's APPI, applies explicitly to any controller who processes PI obtained from EU citizens, whether the controller has a physical presence in the EU or not.[91]

In Article 6, the GDPR lays out six specific instances in which PI processing can be lawful: (1) when the data subject has given consent to the processing for a specific purpose or purposes; (2) when processing is necessary pursuant to a contract between the processor and the data subject; (3) when the controller is under a legal obligation to process the PI; (4) when the PI must be processed to protect the life or safety of the data subject; (5) when the processing is "necessary for the performance of a task carried out in the public interest" or by an official with lawful authority; and (6) where the processing is necessary for the controller to pursue "legitimate interests" as balanced against the rights of the data subject.[92]

The GDPR provides a number of rights for data subjects. Chapter III is dedicated solely to laying out these enumerated rights and the modalities for exercising them. These enumerated rights include the right to transparency in information about PI processing,[93] the right of a data subject to receive and review information that has been collected about them,[94] the right to demand correction of inaccurate information in data collected,[95] and the "right to be forgotten," or, in other words, the right to demand that a company holding an individual's PI delete that information.[96]

Along with all the data privacy regimes reviewed in this note, the GDPR places a range of responsibilities on those processing PI. The regulation requires that controllers have "appropriate" privacy security measures in place to protect processed PI,[97] but it is important to note that individual companies can comply with the GDPR even if their country of origin does not have privacy laws similar to the GDPR in place. Article 7 describes the contours of the GDPR's definition of "consent."[98] In particular, consent must be "as easy to withdraw as to give" and, when consent is given in a written document, the provisions dealing with consent must be separated from other provisions and presented in "clear and plain language."[99] Article 30 requires that

91. *Id.*
92. *Id.* at 36.
93. *Id.* at 39.
94. *Id.* at 40.
95. *Id.* at 43.
96. *Id.*
97. *Id.* at 48.
98. Abigayle Erickson, *Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD*, 44 BROOK. J. INT'L L. 859, 880 (2019).
99. 2016 O.J. (L 119) 37.

controllers "maintain a record of processing activities under its responsibility."[100] If controllers use a new technology to process PI, they must conduct a "data protection impact assessment," and, if that assessment shows that security risk to PI is high, the controller must consult with the "supervisory authority" before moving forward with processing.[101]

The GDPR, China's Law and Standard, Japan's APPI, and California's CPPA espouse many of the same principles and work similarly to obtain their stated policy goals. All four regulations recognize consumers' rights to control and access their personal data; place heavy responsibilities on entities in the business of collecting, processing, and selling PI; and implement vehicles for their respective governmental agencies to establish best practices in security for the retention and transfer of PI.

## II. COMMON DRAWBACKS

Each of the privacy regimes discussed (with the exception of the US federal data privacy regime, or lack thereof) unquestionably provides private citizens with more protection over their PI. By moving beyond the modality-, content-, and child-safety-focused laws that characterize the US federal PI privacy regime, the CCPA, China's Law and Standard, the APPI, and the GDPR each define data collectors, brokers, and processors broadly enough to catch almost any PI-related business activities. However, this wide net may come with considerable costs to companies that participate in and rely on smooth, readily available transborder data flow. The increasing importance of Big Data in business will force countries to continue attempting to balance their legitimate concerns about their citizens' safety and privacy with encouraging business efficiency, growth, and innovation in their economies.

This section explores the drawbacks associated with four common themes in the data privacy regimes discussed above: data localization requirements, requirements for continual consumer consent, the wide reach of internationally operable data laws, and the prolific granting of consumer rights in PI.

---

100. *Id.* at 50.
101. *Id.* at 53-54.

*Data Localization*

Data localization is the practice of "confin[ing] data within a country's borders . . . ."[102] Of the regulations within the scope of this note, only China's Law and Standard explicitly require data localization.[103] However, the infrastructure requirements of both the GDPR and the APPI could lead to increased data localization in those jurisdictions.

Data localization proponents generally claim that the practice ensures increased government control over the privacy and security measures used to protect citizens' PI.[104] Further, data localization policies allow sovereign bodies to provide protection that reflects their constituencies' values, rather than leaving the protection of their citizens' PI up to the privacy policies of businesses across the world who collect, analyze, and sell data.

Unfortunately, due to the fundamental nature of data, data localization may not actually provide the security benefits its proponents espouse. Essentially, this argument is based on the proposition that data hacks can happen anywhere and that keeping data physically in a particular location does not significantly lower the chance that PI will be misappropriated, stolen, or mishandled.[105] Along with, in the best-case scenario, a negligible increase in data security, data localization could also result in higher costs and less data security for businesses. For example, data localization laws significantly hinder the benefits of modern cloud-based data storage, including increased security and lower cost.[106] Leviathan Security Group estimates that companies in countries that choose to impose data localization laws will pay "30-60% more for their computing needs than if they could go outside the country's borders."[107] Additionally, data that is stored on multiple continents simultaneously is safer from infrastructure failure in one particular storage location.[108]

Moving beyond the increased costs to nationally contained businesses, data localization practices necessarily impose increased costs on businesses engaged in transborder data flow. The

---

102. NIGEL CORY, CROSS-BORDER DATA FLOWS: WHERE ARE THE BARRIERS, AND WHAT DO THEY COST? 2 (Info. Tech. & Innovation Found. ed., 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

103. *See* Creemers et al., *supra* note 47.

104. *See* CORY, CROSS-BORDER DATA FLOWS, *supra* note 102, at 3.

105. *Id.* at 4.

106. *See* LEVIATHAN SEC. GRP., QUANTIFYING THE COST OF FORCED LOCALIZATION 2-3 (2015).

107. *Id.* at 3.

108. *Id.* at 2.

implementation of impact statements in the GDPR,[109] for example, imposes costs on firms that are required to create these statements, ostensibly forcing these firms to hire staff, create procedures, and cultivate expertise in this area of regulatory compliance. An empirical study on the economic gains that could be attained from relaxing data localization requirements for transfers between EU member countries estimates GDP increases for member countries as high as 0.18%.[110] A study conducted by the International Trade Commission concluded that US GDP would increase from 0.1-0.3% in "seven digitally intensive sectors" if digital trade barriers like data localization requirements were removed.[111]

While these empirical findings are informative, numbers and projections lend little to our understanding of the pragmatic problems and barriers that data localization presents. A look at Japan's APPI provides an opportunity to examine these issues in a more tangible way. Similar to the GDPR, the APPI does not explicitly require data localization, but its provisions surrounding the transmission of data could result in increased data localization and, arguably, less economically viable trade activity. For example, an American PI company not headquartered in California may not initially be equipped with security infrastructure sufficient to meet APPI's standards.[112] If the company decides that the costs of implementing sufficient infrastructure outweigh the benefits of doing business in Japan, that company will effectively be frozen out of the Japanese PI economy. However, companies located in Japan will have already taken on the costs of implementing adequate security measures since, for them, the cost of insufficient infrastructure would be not doing business at all. This places Japanese PI companies at a natural advantage and could increase the amount of PI held in Japan by increasing the market share of Japanese PI companies.

To summarize, data localization requirements impose higher costs on both local and international businesses with the potential for significant negative impacts on data security. In the context of the goals espoused by the data privacy regimes in this article, data localization requirements fundamentally misunderstand the economics of data and are likely to be ineffective in making PI safer.

---

109. 2016 O.J. (L 119) 53-54.

110. MATTHAIS BAUER ET AL., UNLEASHING INTERNAL DATA FLOWS IN THE EU: AN ECONOMIC ASSESSMENT OF LOCALISATION MEASURES IN THE MEMBER STATES 11 (European Ctr. For Int'l Pol. Econ. eds., 2016).

111. CORY, CROSS-BORDER DATA FLOWS, *supra* note 102, at 8.

112. Those in California would likely have infrastructure that is anticipatorily compliant with the CCPA, which likely meets APPI's standards.

*Requirements for Consent*

The CCPA, China's Law and Standard, the APPI, and the GDPR all impose comprehensive requirements for businesses collecting, selling, and processing PI to gain data-subject consent. China's Law and Standard[113] and the APPI[114] require businesses to obtain continuous consent as they process, sell, and disclose data subjects' PI. The argument in favor of these requirements is clear cut: if the government requires businesses to obtain explicit, ongoing consent from data subjects, individuals will be able to better police the use of their PI over time. Further, holding companies accountable for acquiring consent on an ongoing basis could help improve public trust that these companies are "processing data responsibly."[115]

As with data localization, opponents of strict consent requirements cite economic feasibility and compliance costs as potential downsides.[116] Businesses incur costs in establishing infrastructure both to obtain consent from all data subjects and to track data collected from a particular data subject throughout its digital life cycle.[117] For example, when a company collects PI from data subjects in Japan, it must find a way to attach an individual identity to each piece of data collected to ensure the company can contact the data subject if the scope of PI use changes. The company then must rigorously monitor the use of each of those pieces of data and regularly compare its current use with the use pretext under which the company originally collected it. Because of the volume of data many multinational companies collect, they will need robust systems in place to automatically engage with potentially affected data subjects and reobtain their consent when that subject's data is transferred, reused, or repurposed. This process will likely require companies to incur substantial expenditures on infrastructure, staff, and expertise. For small and mid-sized firms, these costs could price them out of foreign markets completely.[118]

---

113. Mingli, *supra* note 58, art. 5.3.

114. Coos, *supra* note 72.

115. CTR. FOR INFO. POL'Y LEADERSHIP, THE CASE FOR ACCOUNTABILITY: HOW IT ENABLES EFFECTIVE DATA PROTECTION AND TRUST IN THE DIGITAL SOCIETY 24 (2018).

116. *See* MATTHAIS BAUER ET AL., THE ECONOMIC IMPORTANCE OF GETTING DATA PROTECTION RIGHT: PROTECTING PRIVACY, TRANSMITTING DATA, MOVING COMMERCE 4 (European Ctr. For Int'l Pol. Econ. ed., 2013).

117. *See, e.g.*, CAL. CIV. CODE § 1798.135 (West 2020) (requiring businesses that must comply with Section 1798.120 to "provide a clear and conspicuous link on the business's Internet homepage . . . that enables a consumer . . . to opt-out of the sale of the consumer's personal information.").

118. *See* CORY, CROSS-BORDER DATA FLOWS, *supra* note 102, at 2.

*Wide Reach*

California's CCPA, China's Law and Standard, Japan's APPI, and the EU's GDPR all reach across borders and apply to foreign businesses that interact with their respective citizens. While these wide nets provide increased protection to citizens who almost certainly interact with international data collection and sales companies, they could also impose high compliance costs on businesses around the globe.

This note proposes that California's CCPA, in part, is intended to fill the gaps left by the US's piecemeal federal privacy regime. The US's federalist system offers a unique, contained example of the potential costs of geographically varied data privacy regimes. As noted above, the CCPA applies to any company that does business in California.[119] This means that, because of the nature of online data collection, the businesses affected do not have to be headquartered in California or even have any physical presence in the state. Businesses fall under the purview of the statute as soon as they make contact with any California citizen or their PI. If each of the fifty US states enacts laws similar to California, with differences based on their citizens' values and the impact on businesses in each state, data collectors and sellers will be forced to deal with each state's laws individually. Arguably, this will increase the costs of compliance for these businesses.[120] This may explain, in part, why California's statute is limited to businesses that either make a certain dollar amount per year or collect large amounts of data from consumers. In this way, the California legislature has shifted the financial burden of dealing with their regulations to those most able to shoulder it—businesses that make a lot of money.

China's Law and Standard is similarly limited to large businesses, but the international reach of the Law and Standard's jurisdiction presents unique problems for those businesses. Specifically, data companies are concerned about the Law's inspection requirements since the companies may be required to disclose proprietary information to the Chinese government in the process.[121] Further, trade associations can request spot inspections, which raises concerns about the use of the Law as an improper avenue for competitive underhandedness.[122]

---

119. *Id.* at 2.

120. *Id.*

121. Wagner, *supra* note 51 ("The law has raised concerns among some foreign companies over greater data controls as well as increased risks of intellectual property theft.").

122. *See id.* ("Several of the provisions . . . have become a cause for concern among foreign companies. Regarding requirements for spot-checks and certifications, international law firms have warned that companies could be asked to provide source code, encryption, or other crucial information for review by the authorities, increasing risk

International data policy expert Nigel Cory pointed out that Chinese standards, like the Standard discussed in this note, are often characterized by government review and approval for private action and enable the Chinese government to decide how foreign actors can transfer data across China's borders.[123] Cory argues that China's new regulatory scheme could have a significant impact on cross-border data flow since China's standards historically favor domestic industry and products.[124] Thus, while both the CCPA and the Law and Standard's regulations pose problems from a purely administrative and infrastructural standpoint, the Law and Standard add a threat to intellectual property that will have to be carefully considered by businesses interested in doing business in China. It is not out of the question that some companies will, in the face of these concerns, opt not to do business in China at all. On a global scale, a variety of data privacy regimes that cast wide nets would only increase the complexity of navigating these kinds of problems.

*Users' Rights to their Own Data*

The CCPA, China's Law and Standard, the APPI, and the GDPR all grant data subjects certain rights in their PI, for example, the GDPR's "right to be forgotten." At bottom, this proposition is based on the idea that PI is a form of personal property to which rights attach by operation of law.[125] In the US, property rights typically include the right to possess, use, and dispose.[126] As a representative example, these ideas are reflected in the GDPR's right to obtain your data from PI companies through requests for disclosure (possess), the right to decide to whom your data is disclosed (use), and the right to demand deletion of your PI at any time (dispose).

These governments' decisions to grant individual rights in PI create stark economic concerns. The costs incurred by companies to comply with demands for deletion and disclosure alone will likely be

---

of this information being lost, passed on to the local competitors, or used by the authorities themselves.").

123. *See* NIGEL CORY, THE TEN WORST DIGITAL PROTECTIONISM AND INNOVATION MERCANTILIST POLICIES OF 2018 7 (Info. Tech. & Innovation Found. ed., 2019), https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018.

124. *Id.* at 7.

125. *See* SUSAN ARIEL AARONSON, DATA IS DIFFERENT: WHY THE WORLD NEEDS A NEW APPROACH TO GOVERNING CROSS-BORDER DATA FLOWS 6 (Ctr. for Informational Governance Innovation eds., 2018).

126. Newman v. Sathyavaglswaran, 287 F.3d 786, 795 (9th Cir. 2002) (quoting United States v. Gen. Motors Corp., 323 U.S. 373, 378 (1945)).

substantial. Companies must implement a separate infrastructure to shoulder the costs of receiving, processing, sifting, and acting on requests for disclosure and deletion, as they do with localization and consent. Some firms may be forced to charge for what are now nominally free services to offset these new compliance costs.[127] Additionally, these companies will face vastly increased transaction costs anytime they transfer data to third parties, since they will be required to engage with data subjects to obtain consent if the scope of the originally given consent was not sufficiently broad.

## III. COMMON BENEFITS

While it is important for countries formulating data privacy regimes to consider the broad economic impacts any particular set of policies may have, it is also important to balance economic concerns against the privacy and safety of citizens. By granting consumers broad rights to PI, governments around the world are giving consumers a toolbox to protect themselves against exploitative and dangerous data collectors and sellers. This level of protection, albeit potentially cumbersome, is not to be undervalued. Stories like Xu Yuyu's are, unfortunately, not unique. As the number of citizens across the globe who connect to the internet increases, so too does the number of potential victims of invasions of privacy and identity theft.

This section broadly summarizes the arguments in favor of national data privacy regimes as opposed to an international framework, focusing on the societal benefits of nationally varied data privacy schemes from a consumer perspective, including increased personal privacy, the preservation and reflection of local values in data privacy laws, and the potential for reducing illegal data flow.

### *Personal Privacy*

Regions that have enacted more restrictive personal data laws espouse their positive effects on personal privacy. The gaps in the US federal data privacy scheme present a representative example of public policy concerns surrounding inadequate privacy protections for data subjects. The implementation of comprehensive privacy protections for citizens holds companies that deal with PI accountable for their actions. In contrast to Japan's APPI, the US federal data privacy regime does not create a default cause of action for data subjects whose PI is lost in a data breach. Consequently, when a breach occurs, citizens may be left

127. AARONSON, *supra* note 125, at 6.

with no legal recourse. This inevitably leads to a cost shift from the companies, which would be required under a more stringent privacy regime to account for losing PI, to the consumers who are now at increased risk for identity theft and its accompanying financial consequences.[128] This is especially true for companies that do not operate in areas that are typically regulated by federal laws like HIPAA and the FCRA.[129] Without a more comprehensive federal data privacy regime, US consumers are at the mercy of some of the largest data collectors in the world—for example, social media companies like Facebook, search engines like Google, and online marketplaces like Amazon.[130]

In light of these concerns, consumers want more protection.[131] This desire for protection is based partially on the potential financial consequences of a breach,[132] but it is also rooted in the fact that data collectors can reach into data subjects' lives in intimate ways through predictive analysis.[133] Programs like the CCPA, China's Law and Standard, APPI, and GDPR provide safeguards in response to these concerns through their instillation of consumer rights and requirements that data companies disclose the purposes for data collection as a prerequisite to obtaining consent from data subjects. As lawmakers across the world consider the contours of their own countries' data privacy schemes, the economic impact of any given regulation should be balanced against the costs, both financial and emotional, to consumers that follow from inadequate personal privacy protections.

*Preserving Local Values*

National data privacy schemes allow national sovereigns to reflect their constituencies' policy preferences and values. Different cultures value different aspects and facets of privacy. With ever-increasing global use of the internet by both consumers and industrial players, the ability of governments to enact the will of their constituencies becomes increasingly important.

---

128. *See Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL., (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

129. *See* Carol Li, Note, *A Repeated Call for Omnibus Federal Cybersecurity Law*, 94 NOTRE DAME L. REV. 2211, 2213-15 (2019).

130. *Id.* at 2214.

131. *Id.* at 2212.

132. *Id.* (explaining the average cost of each record stolen or lost in a data breach is $148).

133. *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV 93, 94-95 (2014).

In economic commentaries on data privacy regimes, this perspective is often left out. Although economic concerns are always important to consider, so are the unique positions of national governments and the citizens they oversee. As discussed above, California's passing of the CCPA provides a strong example of this principle at work. While the US's lack of comprehensive federal regulation may be due in part to the slow-moving federal legislature, it may also be due to a lack of country-wide pressure from citizens on federal representatives to pass comprehensive data privacy legislation. California, through its ballot initiative mechanism, was able to examine the values of its citizens and enact a data privacy law that mirrored those values. However, the rest of the country may not share these views. Other states have the same authority to pass laws similar to the CCPA, but none have done so to date. Applying this principle globally, a focus on nationally-held values and traditions may put a considerable barrier in the way of unified global data privacy governance. It is likely that sovereigns will want continued control over how their citizens' data is collected, analyzed, and sold so as not to betray their citizens' interests to the interests of international business.

There is, however, an issue with the accuracy of these reflections in countries that do not highly value the democratic process and that may enact data laws to further national economic interests ahead of the interests of their citizens. For example, China's Law and Standard, as discussed above, have been the subject of criticism based on the Chinese government's ability to use the regulations to disadvantage foreign firms and procure proprietary security information. When countries pass laws that focus more on state interests than the interests and values of their citizens, the citizens will likely suffer from decreased foreign firm interaction in their country. China's Great Firewall—designed to keep politically harmful information out of the hands of end users—presents a good example. While the firewall's protection against foreign "bad actors" does in some sense make citizens safer, citizens are also harmed by their lack of access to globally disseminated information.

*Reducing Illegal Data Flow*

Illegal activity is an ever-present concern with unregulated international data flow. Some commentators call for deep levels of interoperability between national and international law enforcement to ensure that data flow stays open and efficient for law enforcement

purposes.[134] Inefficiency, jurisdictional confusion and disagreement, and "data havens" have caused consternation in investigations of international financial institutions, child pornography distribution, and online human trafficking rings.[135] Interoperability in national data privacy regimes could help both international and domestic law enforcement agencies more efficiently pursue criminals who move data across borders.

Data localization naturally presents a barrier to efficient law enforcement by providing digital "lockboxes" to criminals savvy enough to transfer their data into countries with high borders around data. For example, a criminal enterprise in the US could move illegal data onto a Chinese server. If US law enforcement, in the course of an investigation, attempts to obtain the data, it is likely that, at minimum, the requirements in China's Law and Standard's requirements for security infrastructure verification and institutional spot checks would slow the data transfer process. By the time US law enforcement officers got their hands on the data they were looking for, the trail may well have gone cold. Interoperability and an application of Prime Minister Abe's principles of trust in data flow internationally, especially in the context of illegal data, could go a long way to making this process run more smoothly.

These arguments meet considerable opposition, however, from commentators concerned about foreign government access to domestic citizens' PI. Using China's Law and Standard again as an example, there are already concerns about opportunities for abuse by Chinese industry in enabling trade associations to request investigations into foreign firms' security infrastructure. It follows that countries with motives contrary to the principle of upholding the law internationally could use open international law enforcement channels to illicitly gather data on other countries' citizens.

## IV. POTENTIAL SOLUTIONS

This section presents a brief overview of potential solutions to the economic and social challenges global data privacy regimes present. These suggestions are meant to be succinct, and any one of them could be (and have been) the subject of their own dedicated academic writing.

134. CORY ET AL., *supra* note 69, at 14-15.
135. *Id.* at 18-19.

*International Frameworks*

Some commentators call for international frameworks that would promote more uniform data governance, exceptions from strict regulatory schemes for certain kinds of data, and interoperability in data regulation schemes in law enforcement.[136] An internationally agreed-upon scheme has obvious benefits, particularly for multinational businesses. Compliance costs would be much lower for multinational firms that only have to deal with implementing sufficient infrastructure to deal with one unified data privacy framework.[137] A unified framework would remedy issues with, for example, GDPR and APPI requirements for third-party security infrastructure. It would save businesses money on things like impact statements, which would be unnecessary if the globe's data privacy regulations were standardized. Finally, an international framework could include specific, expedited data transfer provisions for national and international law enforcement, with safeguards against misuse of law enforcement channels for illicit foreign data collection.

The drawback is that these kinds of agreements are notoriously difficult to negotiate, fraught with political posturing, and historically lacking in enforcement mechanisms. As evidenced by the world's attempts to decide on a global governance regime for climate change, data presents a similar global governance problem. As discussed above, citizens across the world value privacy differently. Sovereigns want to reflect those values while promoting their own national industrial and economic growth. Some, like California, lean on the side of the citizens' values, while others, like China, lean on the side of state interests. These differing values, morals, and goals will likely stymie any attempts at broad international frameworks in the near term.

*Limits on or Avoidance of Data Localization*

Data localization presents one of the largest hurdles to the free flow of data internationally. It not only presents problems from a consumer and industrial perspective, but also might not actually increase privacy protections in countries that implement it. As noted above, the physical location of data does not necessarily improve its safety. Hackers and identity thieves exist in every country in the world, and they will access data stored in one country as readily as they will access data stored in another. In short, data localization imposes costs on foreign businesses

136. *See id.* at 6.
137. *See* CORY, CROSS-BORDER DATA FLOWS, *supra* note 102, at 11.

attempting to interact economically with countries with data localization requirements and on citizens in countries with high data borders who cannot access the full breadth of information the global internet provides.

*Exceptions for Health Research Data*

A major argument for the free flow of data focuses on health-based innovation. The idea is, if health-related data were widely available, research institutions and industrial pharmaceutical companies would have more to work with when developing solutions to the world's health problems. The ever-present individual privacy concern rears its head here perhaps more than anywhere else, however, because citizens across the globe place a high value on the privacy of their health-related information. HIPAA presents a good working example of the public policy concerns surrounding the privacy of health data because it requires stringent security measures and de-identification practices surrounding health data's transfer.

In the end, a robust interoperable international system for sharing health information in a standardized format (similar to that proposed for law enforcement in this note) could provide benefits with the use of encryption and anonymization to reduce public information disclosure concerns. As with illegal international data investigations, health data could cause concern about foreign meddling in individuals' health data for nefarious purposes. International agreements to trade health data with efficient safeguards and restrictions could shore up many of these concerns through thorough third-party recipient vetting, purposeful disclosure requirements (like those contained in the GDPR and APPI), and consent requirements for companies that wish to transfer patients' health data internationally.

*Continuing with Business as Usual*

International data governance *is* international trade governance. While our international commodity trade scheme is far from perfect, historically, trade between countries has continued except in times of heightened international strife and disagreement. As data flow continues to become more integral to international business, countries and companies will be forced to confront problems with varied international schemes head on.

Arguably, the weight of the cost of international data compliance is best left with large, multinational companies that can afford it. This argument is reflected in the provisions in the CCPA and China's Law

and Standard that set minimum requirements for the level of business and data activity that companies must meet for these laws to apply to them. By shifting the burdens of compliance to companies that can best afford them, these laws accomplish two goals: first, consumers are not left with the costs of data breaches and vulnerability in the storage and transfer of their PI and, second, small and mid-sized firms are still able to participate in foreign data trade and transfer without being priced out by stringent compliance requirements.

Based on the economic reality that many strict data privacy regimes will have negative economic impacts on national economies, it follows that large businesses in these economies will eventually be incentivized to work together to create comprehensive compliance packages to deal with varying national standards. Eventually, after the dust settles, dealing with data trade regulations will take the same form as dealing with international trade regulations: though potentially costly and sometimes cumbersome, a necessary and palatable expense of doing business.

## CONCLUSION

There is a wide range of influences on international data governance. On the whole, a system that protects personal data, preserves national security, and promotes the free flow of industrial and innovative data could be in reach. Through a combination of increased interoperability for international law enforcement, minimization of data localization provisions, and provisions requiring businesses to be a certain size before data privacy laws affect them, governments could achieve a tenuous balance between privacy and economic growth.

While this process will be aided by international cooperation, the process may be best left alone at the international level. The incentives for nationally-contained data governance laws are too strong for anyone to predict with any confidence whether countries will choose a globally standardized privacy framework over enacting their own specific legal frameworks. While this may present problems in the short term, firms will inevitably grow and change to accommodate new data privacy laws and, in the end, we will be left with a global data privacy regime that reflects local values, encourages responsible business growth and innovation, and provides consumers and data subjects with more robust protections and the peace of mind that comes with them.