Richmond Journal of Law & Technology Volume XXVII, Issue 2

A RISING TIDE LIFTS ALL CONSUMERS: PENUMBRAS OF FOREIGN DATA PROTECTION LAWS IN THE UNITED STATES

Michael P. Goodyear*

Cite as: Michael P. Goodyear, *A Rising Tide Lifts All Consumers: Penumbras of Foreign Data Protection Laws in the United States*, 27 RICH. J.L. & TECH., no. 2, 2020.

* J.D., University of Michigan Law School (2020); A.B., University of Chicago (2016). Thanks are due to Lori Andrews for her constantly helpful advice, friendship, and mentorship, both on this article and in the law.

ABSTRACT

With the growth of collecting, processing, and transferring personal information to third parties, consumers' data is increasingly exposed to a myriad of risks. Perhaps chief among these are the data protection practices of data collectors themselves. Yet despite the risk to consumers, U.S. data protection law has remained fragmented, focused on individual industries at the federal level and only comprehensive, occasionally, at the state level. This lack of a comprehensive data protection law in the United States is a significant detriment to the security of U.S. consumers. International law also fails to offer a path that could comprehensively protect U.S. consumers.

Yet U.S. consumers' personal information receives protections from an unlikely source: foreign data protection laws. There is a growing global trend to adopt comprehensive data protection laws, with the European Union, Brazil, Japan, and others adopting such legislation in the past few years. This article examines nine of these laws from five different continents, looking at the global trends and disparities shown by thissample. The influence of these nine laws and other legislation creates distinct soft law benefits for U.S. consumers. They do this chiefly through applying economic pressure to U.S. data collectors to adopt a one-size-fits all approach, social pressures from increased privacy awareness by consumers, political pressures for the U.S. to adopt equivalent national legislation, and practical benefits from having a variety of different foreign models to observe and select. While reliance on foreign data protection lawsdoes not completely substitute for the United States adopting its own comprehensive federal data protection laws, the penumbras that spill over from foreign data protection laws offer largely unexamined, but significantbenefits for U.S. consumers.

I. INTRODUCTION

[1] Snapchat accesses its users' contacts and photos.[1] The Weather Channel app tracks your exact location.[2] Duolingo has access to yourcamera and audio.[3] While these functions may seem innocuous, behind the scenes, mobile applications and websites are collecting, processing, and sharing consumers' personal information with third parties.[4] Consumers conducting more of their daily lives online has acerbated this trend.[5] The incentive is obvious: the personal data market is worth billions and is expected to grow to $200 billion by 2022.[6] Yet despite the size and power of the personal data market, not to mention platforms and applications' control over intimate and private details, the United States only has a fragmented series of data protection laws that allow large loopholes for data

[1] *Privacy Policy*, SNAP INC. (Sept. 14, 2020), https://snap.com/en-US/privacy/privacy-policy [https://perma.cc/WW53-SPDP].

[2] *See Privacy Policy*, THE WEATHER CHANNEL (Dec. 29, 2019), https://weather.com/en-US/twc/privacy-policy [https://perma.cc/RP9B-8Y3B].

[3] *Privacy Policy*, DUOLINGO (Oct. 11, 2018), https://www.duolingo.com/privacy [https://perma.cc/6TUE-JNAX].

[4] *See* Nick Statt, *Some Major Android Apps Are Still Sending Data Directly to Facebook*, THE VERGE (Mar. 5, 2019 7:41 PM), https://www.theverge.com/2019/3/5/18252397/facebook-android-apps-sending-data-user-privacy-developer-tools-violation [https://perma.cc/9WB8-97YE] (finding that a number of apps, including Yelp, Duolingo, and two Muslim prayer apps, send user data to Facebook); *'Tracking Every Place You Go': Weather Channel App Accused of Selling User Data*, THE GUARDIAN (Jan. 4, 2019 9:39 PM), https://www.theguardian.com/ technology/2019/jan/04/weather-channel-app-lawsuit-location-data-selling [https://perma.cc/W22R-PRCV].

[5] *See* Michael Goodyear, *The Dark Side of Videoconferencing: The Privacy Tribulations of Zoom and the Fragmented State of U.S. Data Privacy* Law, 10 HOUS. L. REV. 76, 79 (2020) (describing privacy concerns associated with using the video-conferencing software Zoom).

[6] Rana Foroohar, *How Much Is Your Data Worth?*, FIN. TIMES (Apr. 8, 2019), https://www.ft.com/content/3f2b0f0e-57cc-11e9-91f9-b6515a54c5b1 [https://perma.cc/XPW4-UZN3].

collectors.[7] The United States does not have a comprehensive federal data protection law, and the federal and state laws that do exist result in an inadequate patchwork that does not adequately, or equally, protect U.S. consumers.[8]

[2] Because of the shift in how U.S. consumers conduct their daily lives, their personal data is in a dire state. Terms concerning personal data collection are buried in opaque (and sometimes purposefully obfuscated) privacy policies[9] that would take days, if not weeks, to read in the aggregate.[10] Even when companies have privacy policies in place, these

[7] *See generally* Florian Schaub, *Fragmented U.S. Privacy Rules Leave Large Data Loopholes for Facebook and Others*, SCI. AM.: THE CONVERSATION (Apr. 10, 2018), https://www.scientificamerican.com/article/fragmented-u-s-privacy-rules-leave-large-data-loopholes-for-facebook-and-others [https://perma.cc/L89U-C2L4] (noting that U.S. privacy laws are mostly based on FTC practice principles and fail to provide a comprehensive privacy regime).

[8] Sean Hackbarth, *'A Patchwork is Not Acceptable': Making the Case for a National Privacy Law*, U.S. CHAMBER OF COMMERCE: ABOVE THE FOLD (July 29, 2019 9:00 AM), https://www.uschamber.com/series/above-the-fold/patchwork-not-acceptable-making-the-case-national-privacy-law [https://perma.cc/Q9XG-TBWH] (referring to the patchwork of federal and state laws as inadequate for protecting U.S. consumers); Goodyear, *supra* note 5, at 89 (arguing that the greater protections of the California Consumer Privacy Act, compared to those in other states, create disparate data privacy rights for different groups of Americans).

[9] Joseph Bonneau & Sören Preibusch, *The Privacy Jungle: On the Market for Data Protection in Social Networks*, *in* 8 ECONOMICS OF INFORMATION SECURITY AND PRIVACY 121 (Tyler Moore et al. eds., 2010) (arguing that websites specifically make their privacy policies difficult to read so that users do not know what privacy is offered); *see* Alexander Tsesis, *Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure*, 90 UNIV. COLO. L. REV. 593, 597–98 (2019) (noting Google and other major platforms' terms); Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html [https://perma.cc/M4RG-2M7V].

[10] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543, 563 (2008) (finding that it would take

companies still frequently engage in poor privacy practices.[11] Some companies require far more data and permissions than could possibly be necessary for their applications to function.[12] In other cases, companies even fail to follow their own privacy practices.[13] Furthermore, consumers are often unaware of these obfuscated practices that target their intimate and personal information.[14] With limited government regulations, consumers are left at least partially exposed to the privacy whims of data collectors.[15]

an individual forty minutes a day to read the privacy policies of routinely used online services); Keith Wagstaff, *You'd Need 76 Work Days to Read All Your Privacy Policies Each Year*, TIME (Mar. 6, 2012), https://techland.time.com/2012/03/06/youd-need-76-work-days-to-read-all-your-privacy-policies-each-year [https://perma.cc/7B35-WZ3J].

[11] *See* Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 438 (2018); *see e.g.*, Goodyear, *supra* note 5, at 78–80 (examining Zoom's privacy practices).

[12] Andrews, *supra* note 11, at 439–40 (noting that the number of "overprivileged" mobile health apps is high, with, for example, an app that displays recipes requiring permissions to "find user accounts on the phone; read and modify contacts; read the calendar; track the user's precise (GPS-based) location; make phone calls; read and modify the call log; test access to and modify external storage; obtain the device ID; activate the camera and microphone, and install and delete other applications").

[13] *See, e.g.*, Tsesis, *supra* note 9, at 597 (noting how Google and other platforms have misled consumers about how they use their tracking functions).

[14] *Id.*

[15] *See* Brianna Provenzano, *While Europe Cracks Down on Data-Collection Practices, U.S. Consumers Remain as Vulnerable as Ever*, PACIFIC STANDARD (Jan. 29, 2019), https://psmag.com/economics/france-fines-google-data-protection [https://perma.cc/E5AR-JSYB] (describing how a lack of regulatory oversight in the U.S. allows companies to "compile data sets of where a person goes, who they talk to, and what they buy with relative impunity").

[3] While a comprehensive federal data protection law that could better protect U.S. consumers has not been forthcoming[16]—and an international legal framework on data protection is practically nonexistent[17]—progressively more stringent data protection laws have been enacted in increasing numbers in countries around the world over the past few years. This effort has been led by the European Union's ("EU") General Data Protection Regulation ("GDPR").[18] Scholars have examined how U.S. companies have complied with the GDPR,[19] how the California Consumer Privacy Act was influenced by the GDPR,[20] how individual countries have navigated data negotiations with the EU,[21] how the GDPR has significantly

[16] *See* STEPHEN P. MULLIGAN ET AL., CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 51–52 (2019) (describing the Trump Administration's criticisms of a national data protection law like that of the GDPR). *But see* Lucas Ropek, *Privacy Policy and the Biden Presidency: A Promising Outlook?,* GOV. TECH. (Dec. 10, 2020), https://www.govtech.com/security/Privacy-Policy-and-the-Biden-Presidency-A-Promising-Outlook.html [https://perma.cc/PLL4-C5TV] (concluding that a federal data privacy law is perhaps likely under the Biden administration).

[17] *See* discussion *infra* Part II(A).

[18] *See* Enza Iannopollo, *Stringent Data Protection Regulation Has Gone Global*, ZDNET (June 24, 2019), https://www.zdnet.com/article/stringent-data-protection-regulation-has-gone-global/ [https://perma.cc/GA3K-CZN6].

[19] *See generally* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365 (2019); Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J. L. & TECH. 1 (2018).

[20] Rustad & Koenig, *supra* note 19, at 403–04 (discussing similarities between the California Consumer Protection Act and the GDPR).

[21] *See e.g.*, Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 783–803 (2019) (discussing the adequacy model of Japan and the bilateral negotiations of the United States).

[22] *See generally* Orin Pietersen, Externalization of the GDPR: Promoting Global Regulatory Standards in Data Protection and Privacy (June 10, 2018) (Master thesis, Leiden University) (on file with the Leiden University Repository: Crisis and Security Management) (discussing theories of how GDPR influences data protection worldwide).

influenced the enactment of data protection laws worldwide,[22] and how new models for U.S. data privacy are based on, in whole or in part, the GDPR model.[23] This article takes a different approach, examining the global scale of improved data protection regulations and finding that foreign data protection acts create soft law influences on U.S. data collectors, consumers, and policy makers—creating not insignificant benefits for the privacy of U.S. consumers' personal information.

[4] Part II examines the global context of data protection laws, first reviewing the scant international legal protections for data privacy and then looking at nine of the most sophisticated foreign data privacy laws in the world, those of the EU, Argentina, Brazil, Canada, Israel, Japan, New Zealand, Switzerland, and Uruguay. Next, Part III analyzes the current state of U.S. data privacy law, both at the federal level and state level with the recently enacted California Consumer Privacy Act, comparingboth to the nine foreign privacy law regimes examined in Part II. Part IV examines the distinct soft law benefits that these foreign data privacy laws create for U.S. consumers, chiefly through economic pressures for U.S. data collectors to adopt a one-size-fits all approach, social pressures from increased privacy awareness by consumers, political pressures for the U.S. to adopt equivalent national legislation, and practical benefits from having a variety of different foreign models to observe and select. Part V concludes with the caution that foreign data protection laws cannot fully replace a comprehensive U.S. federal data privacy law, but they can provide soft law coverage of many of the lacunae created by the lack of such a law in the United States.

[23] *See* Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1063, 1081 (2019) ("State legislatures have already begun to emulate certain aspects of the GDPR, and some state constitutions already contain a right to privacy like the one undergirding the European law."); Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1688, 1690–93 & 1713 (2020) (highlighting U.S. states that adopted "mini-GDPR" privacy laws).

II. DATA PRIVACY AROUND THE WORLD

A. International Data Privacy Law

[5] There is no single, global treaty on data protection.[24] There are, however, international instruments and organizations that address the right to data privacy and its protections.[25] The main four entities that address privacy rights are the Human Rights Council, the Organization for Economic Cooperation and Development ("OECD"), the Global Privacy Assembly (formerly the International Conference of Data Protection and Privacy Commissioners), and the Council of Europe's Convention 108.[26]

[6] Privacy is protected under the United Nation's ("UN") human rights treaties.[27] The right of privacy is embodied in both Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.[28] The UN Human Rights Council has interpreted the "right to privacy in the digital age" under the same overarching right to privacy, encouraging states to respect and protect the

[24] U.N. Conference on Trade and Development ("UNCTAD"), *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, 24, U.N. Doc. UNCTAD/WEB/DTL/STICT/2016/1/iPub (2016) [hereinafter UNTCAD].

[25] *See, e.g.*, Clément Perarnaud, *Privacy and Data Protection*, GIP (Oct. 9, 2020), https://dig.watch/issues/privacy-and-data-protection [https://perma.cc/P8XN-S7SC] (discussing international instruments and organizations that address the right to data privacy and its protections).

[26] *See International Privacy Standards*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/international-privacy-standards [https://perma.cc/X5SK-2Q5Q] (listing major intergovernmental entities in data privacy and protection); *Promotion and Protection of Human Rights Around the Globe*, U.N. HUM. RTS.: OFF. OF THE HIGH COMM'R, https://www.ohchr.org/EN/pages/home.aspx [https://perma.cc/645Y-KKHK] (defining the Human Rights Council).

[27] G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948).

[28] *See id.*; G.A. Res. 2200 (XXI) A, International Covenant on Civil and Political Rights, art. 17 (Dec. 16, 1966).

right to privacy online just as they would offline.[29] Furthermore, the Human Rights Council encourages states to "develop or maintain and implement adequate legislation . . . that protects individuals against . . . the unlawful or arbitrary collection, processing, retention or use of personal data by individuals, Governments, business enterprises and private organizations."[30] In 2016, the Human Rights Council even appointed a Special Rapporteur to submit recommendations to the Council on the right to privacy in the Internet age and how to best protect this right.[31] However, these initiatives are highly abstract and serve as broad recommendations, making it difficult to apply such statements to concrete laws or the day-to-day regulation of privacy practices.[32]

[7] Unlike the Human Rights Council, the OECD has provided more specific guidelines, but these guidelines serve merely as recommendations rather than treaty obligations.[33] The OECD has also promulgated a recommended data protection framework,[34] butit is not legally binding.[35] Additionally, only thirty-four countries are

[29] *See* Human Rights Council Res. 34/7, U.N. Doc. A/HRC/RES/34/7, at 1, 4 ¶ 5(a)–(b) (Apr. 7, 2017).

[30] *Id.* at ¶ 5(f).

[31] Human Rights Council Res. 28/16, U.N. Doc. A/HRC/RES/28/16, at ¶ 4(g)–(h) (Apr. 1, 2015); *see also* UNCTAD, *supra* note 24, at 24–25 (explaining that the Special Rapporteur was appointed in July 2015 and submitted his first report in March 2016).

[32] *See* UNCTAD, *supra* note 24, at 25.

[33] *See OECD Privacy Guidelines*, OECD, http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm [https://perma.cc/G4VP-FR97] (explaining that the guidelines are a "set of privacy principles" and that the OECD continues to work on "practical recommendations" for implementation).

[34] *See* ORG. FOR ECON. COOP. & DEV., THE OECD PRIVACY FRAMEWORK 13–17 (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [https://perma.cc/5KAY-6N7D].

[35] *Id.* at 46.

members of the OECD.[36] Even if the OECD had more members, its guidelines have been interpreted as having relatively weak requirements.[37] Lamentably, the 2013 update of the OECD guidelines did not do much to strengthen these requirements.[38]

[8] The Global Privacy Assembly has also entered the international privacy regulation space, issuing a statement on personal data and privacy called the Montreux Declaration.[39] The Montreux Declaration is not binding,[40] nor does it include follow up mechanisms other than the annual meetings of the Global Privacy Assembly.[41]

[9] Unlike the OECD and the Global Privacy Assembly, the Council of Europe has established binding data protection regulations in Convention 108.[42] Convention 108 provides a stronger standard of privacy protections

[36] *Id.* at pmbl. ("The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.").

[37] *See* GLOB. PRIV. PROT.: THE FIRST GENERATION 167 (James B. Rule & Graham Greenleaf eds., 2008).

[38] Graham Greenleaf, *The UN Should Adopt Data Protection Convention 108 as a Global Treaty: Submission on 'the Right to Privacy in the Digital Age' to the UN High Commission for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy*, 24 UNIV. S. WALES LAW RSCH. SER. (2018), https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/GrahamGreenleafAMProfessorLawUNSWAustralia.pdf [https://perma.cc/R5XN-ENCE].

[39] 27th Int'l Conf. of Data Prot. & Priv. Comm'rs, *Montreux Declaration* (Sept. 16, 2005); UNCTAD, *supra* note 24, at 27.

[40] *Montreux Declaration*, *supra* note 39.

[41] UNCTAD, *supra* note 24, at 27.

[42] *See id.* at 25.

than the OECD guidelines, and an additional protocol added in 2001 further modernized these standards.[43] Convention 108 and its additional protocol are also open to signatures from non-Council of Europemember states. However, adherence by non-member states has not been forthcoming. So far, only eight of the current thirty-five signatories of Convention 108 are not members of the Council of Europe, and two of these non-member signatories have not signed the additional protocol.[44] So, although scholars—most prominently Australian scholar Graham Greenleaf—have called for using Convention 108 as the basis for a truly global treaty on data protection,[45] the lack of enthusiasm from non-European countries undermines the promise of such a proposal.[46]

[10] The lack of international data privacy laws has led to calls for a global treaty on data protection[47] and greater bilateral partnerships between

[43] Greenleaf, *supra* note 38, at 1–2. *See generally* Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows, Nov. 8, 2001, E.T.S. No. 181 (providing the "modernized" language of Convention 108); Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108 (providing the original language of Convention 108).

[44] *Chart of Signatures and Ratifications of Treaty 108*, COUNCIL OF EUR. TREATY OFFICE (Oct. 22, 2020), https://www.coe.int/en/web/conventions/full-list//conventions/treaty/108/signatures [https://perma.cc/E5DH-XYCP]; *Chart of Signatures and Ratifications of Treaty 181*, COUNCIL OF EUR. TREATY OFFICE (Oct. 22, 2020), https://www.coe.int/en/web/conventions/fulllist//conventions/treaty/181/signatures?p_auth=7vbEdAcm [https://perma.cc/D8QU-WUNU].

[45] *See generally* Graham Greenleaf, *A World Data Privacy Treaty? "Globalisation" and "Modernisation" of Council of Europe Convention 108*, PRIVACY IN EUROPEAN HUMAN RIGHTS INSTRUMENTS 92 (Normann Witzleb et al., eds., 2014).

[46] *See generally Chart of Signatures and Ratifications of Treaty 108*, *supra* note 44 (showing that only eight non-European countries have ratified Convention 108).

[47] *See* Greenleaf, *supra* note 45; Morgan A. Corley, *The Need for an International Convention on Data Privacy: Taking a Cue from the CISG*, 41 BROOK J. INT'L L. 721, 766 (2016).

major global players, such as the EU and the United States.[48] Differing national understandings of data privacy are a particularly onerous roadblock standing in the way of an international treaty.[49] And at present, there is no true international binding structure that regulates data privacy laws.[50] Therefore, data privacy regulation is primarily at the national level rather than the international level.[51] However, that is not necessarily a problem. Unlike other areas of the law—say intellectual property, where differing intellectual property regimes cause significant barriers to trade and have prompted complex international treaty regimes,[52]—the Internet, and by extension data of Internet users, is global. This, in turn, means that laws in one country can and will have spillover effects in other countries, in part due to the fact that companies that process personal data operate in multiple jurisdictions, if not on a global scale.[53]

[48] *See generally* Paul M. Schwartz & Karl-Nikolaus Peifer, *Structuring International Data Privacy Law*, *in* 21 INT'L DATA PRIVACY LAW, https://www.law.berkeley.edu/wp-content/uploads/2019/10/Schwartz-Intl-Data-Privacy-Law-21.pdf [https://perma.cc/SAY6-HZ8Z] (arguing that the future of international data privacy depends on the collaboration between the EU and the United States).

[49] Marcin Rojszczak, *Does Global Scope Guarantee Effectiveness? Searching for a New Legal Standard for Privacy Protection in Cyberspace*, 29 INFO. & COMMC'NS TECH. L. 22, 43 (2020).

[50] *See* Corley, *supra* note 47 at 722–23.

[51] *See id.* at 721–22.

[52] *See e.g.*, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, Apr. 15, 1994, 1869 U.N.T.S. 319 (establishing the Agreement on Trade-Related Aspects of Intellectual Property Rights); *see* David Nimmer, *The End of Copyright*, 48 VAND. L. REV. 1385, 1393 (1995).

[53] *See* Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOB. LEGAL STUD. 475, 487 (1998).

B. Comparative Data Privacy Law

[11] While there is no comprehensive international framework for data privacy, most countries have adopted some sort of legislation on data protection.[54] As of December 2020, 132 countries have enacted legislation to protect data privacy,[55] including the majority of UN member states.[56] This is an immense increase from the 1990s, when only twenty countries had such legislation.[57] Today, national data privacy laws cover 66% of countries worldwide.[58]

[12] This article analyzes the main provisions of some of the most stringent data protection laws in the world. It summarizes the laws of nine jurisdictions, starting with the EU and then addressing the largest countries that the European Commission determined have adequate data protection laws (Argentina, Canada, Israel, Japan, New Zealand, Switzerland, and Uruguay), as well as Brazil, whose significant new data privacy law came into effect in 2020.[59]

---

[54] *See* Corley, *supra* note 47, at 722.

[55] *Data Protection and Privacy Legislation Worldwide*, UNCTAD, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx [https://perma.cc/NEB8-XWQA].

[56] *See* Graham Greenleaf, *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*, 145 PRIVACY L. & BUS. INT'L REP. 1, 6 (2017).

[57] Emmanuel Durou, *Big Data: Mining a National Resource*, MIDDLE E. POINT VIEW 23, 26 (2015).

[58] *Data Protection and Privacy Legislation Worldwide*, *supra* note 55.

[59] *See Adequacy Decisions*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/8ENC-FJED]; *BREAKING: Brazilian Data Protection Law Will Soon Come Into Effect*, HUNTON ANDREWS KURTH (Aug. 27, 2020), https://www.huntonprivacyblog.com/2020/08/27/breaking-brazilian-data-protection-law-will-soon-come-into-effect/ [https://perma.cc/RC3K-YR7E].

While there are other countries that also have significant data protection laws, including, *inter alia*, China and Russia,[60] this will serve as an initial sample of economically significant countries across five continentswith strong data protection laws that follow the growing comprehensive data protection law model.

[13] For the purposes of comparing these nine laws, this article examines nine specific questions pertaining to the most significant data privacy requirements addressed in these laws. The nine questions are as follows:

1. What information is protected?
2. How does the law treat anonymous, deidentified, pseudonymous, and aggregated data?
3. What notice requirements are there for consumers?
4. Is consent required for the collection of personal data?
5. Is there a required opt-out right for the sale of personal information?
6. Is there an individual right of access or disclosure of personal information?
7. Is there a right to correct data?
8. Is there a right to delete or erase personal information (a right to be forgotten)?
9. Are there any requirements for the international transfer of data?[61]

[60] *See Data Protection Laws of the World*, DLA PIPER, https://www.dlapiperdataprotection.com [https://perma.cc/8SFC-DKAN].

[61] *See, e.g.*, Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, THOMSON REUTERS (2018), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf [https://perma.cc/8PLZ-F83P] (elucidating important comparative law questions by juxtaposing some of the most important provisions of the California Consumer Privacy Act ("CCPA") and the GDPR).

1. European Union

[14] The EU passed its comprehensive General Data Protection Regulation ("GDPR") in 2016, effective 2018.[62] As EU law, the GDPR applies to all twenty-seven EU member states.[63] The GDPR protects personal data, defined as any information relating to an identified or identifiable data subject that would identify that subject by itself or in combination with one or more factors.[64] It places pseudonymous data within its ambit, but does not consider anonymous data as personal data.[65]

[15] The GDPR provides a series of rights to data subjects.[66] Interms of notice, the GDPR requires data controllers to disclosedetailed information about their personal data collection and data processing activities, including whether the data is collected from the data subject directly or from a third party.[67] Consent must be given by a clear affirmative act, [68] such as ticking a box when entering a website. Despite the absence of an explicit opt-out right, data subjects can withdraw their consent for processing activities,

[62] Council Regulation 2016/679, art. 99, 2016 O.J. (L 119).

[63] *Id.*; *Countries*, EUROPEAN UNION, https://europa.eu/european-union/about-eu/countries_en [https://perma.cc/NG3G-Y2K9].

[64] Council Regulation 2016/679, art. 1, 4(1), 5(1), 2016 O.J. (L 119); *see also id.* art. 9 (including special rules for personal data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership" and the processing of "genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation").

[65] *Id.* recital 26, art. 4(5).

[66] *Id.* recital 11.

[67] *Id.* art. 13(1)–(3), 14(1)–(2), 14(4).

[68] *Id.* art. 6(1)(a), 7.

producing the same result.[69] Data subjects also have the right to obtain access to their personal data from the controller[70] and rectify any inaccurate personal data concerning them.[71] Under certain circumstances, the data subject also has the right to request the erasure of personal data concerning them.[72] Personal data can be moved freely to otherjurisdictions if those jurisdictions have been deemed to have an "adequate" level of data protection by the European Commission,[73] although there are exceptions, including, primarily, if the data subject explicitly consents.[74]

2. Argentina

[16] Argentina's Personal Data Protection Act ("PDPA") became effective in 2000 [75] and is based largely on European privacy principles. Following the enactment of the GDPR, there is also a new bill in front of the Argentine Congress that would bring the Act even more in line with

[69] *Id.* art. 7(3); *see also* Jehl & Friel, *supra* note 61 (comparing opt-out provisions of the CCPA and GDPR based on their functions).

[70] Council Regulation 2016/679, art. 15, 2016 O.J. (L 119).

[71] *Id.* art. 16.

[72] *Id.* art. 17 (providing that a user may request erasure where (a) the personal data is no longer necessary for the purpose for which they were required; (b) the data subject withdraws consent; (c) the data subject objects to the processing; (d) the personal data have been unlawfully processed; (e) the personal data must be erased to comply with a Member State's law; or (f) the personal data have been collected in relation to offering information society services).

[73] *Id.* art. 45(1)–(2).

[74] *Id.* art. 49(1)(a).

[75] LEY DE PROTECCIÓN DE LOS DATOS PERSONALES [Personal Data Protection Act], Law No. 25.326, Oct. 4, 2000 (Arg.); *see* Diego Fernández, *Argentina's New Bill on Personal Data Protection,* IAPP (Oct. 02, 2018), https://iapp.org/news/a/argentinas-new-bill-on-personal-data-protection/ [https://perma.cc/9RPX-ZA3M].

the GDPR.[76] At present, the PDPA protects personal data, defined as information of any kind that refers to ascertainable physical persons or legal entities.[77] This does not apply to data that has been anonymized or disassociated.[78]

[17] Like the GDPR, the PDPA provides a series of rights to data subjects. Data subjects must be informed about the purpose for collecting their personal data.[79] The data subject must expressly consent to the data collector, although there are limited exceptions.[80] Personal data can also only be communicated to third parties if it is for a legitimate purpose for which consent was received from the data subject.[81] The PDPA allows data subjects to withdraw their name and information from sales, advertising, and similar activities.[82] Data subjects have a clear right of access to their collected data,[83] as well as a right to correct or rectify their collected personal data.[84] They also have the right to suppress personal

[76] *Argentina: A Bill Updating the Data Protection Laws was Sent to Congress*, ALFARO ABOGADOS, https://www.theworldlawgroup.com/writable/documents/news/Argentina-Data-Protection-Bill-2020.pdf [https://perma.cc/757X-8Q3R].

[77] LEY DE PROTECCIÓN DE LOS DATOS PERSONALES [Personal Data Protection Act], Law No. 25.326, § 1, 2 (Arg.).

[78] *Id.* at § 11(3)(e).

[79] *See generally id.* at § 6 (outlining notice requirements).

[80] *See generally id.* at § 5 (outlining consent requirements).

[81] *Id.* at § 11(1).

[82] *Id.* § 27(3).

[83] LEY DE PROTECCIÓN DE LOS DATOS PERSONALES [Personal Data Protection Act], Law No. 25.326, § § 14(1) (Arg.).

[84] *Id.* § 16(1).

information upon request, effectively a right to be forgotten.[85] Argentina prohibits the international transfer of data to countries that lack "adequate levels of protection," subject to limited exceptions; but, unlike the GDPR, consent is not an exception.[86]

3. Brazil

[18] Brazil approved its new General Data Protection Law ("LGPD") in 2018, which took effect in August 2020.[87] The LGPD governs the processing of personal data, defined as information regarding an identified or identifiable person.[88] Anonymized data does not qualify as personal data.[89]

[19] Data subjects have the right to know the purpose of processing their data at the time of consent.[90] Processing of personal data generally requires the explicit and informed consent of the data subject, although there are some alternatives.[91] Consent may be revoked at any time, which is effectively the same as an opt out right for sales.[92] The data subject has

[85] *Id.* § 16(2).

[86] *Id.* § 12(1)–(2).

[87] Kate Black et al., *6 Months Until Brazil's LGPD Takes Effect – Are You Ready?*, NAT'L L. REV. (Mar. 5, 2020), https://www.natlawreview.com/article/6-months-until-brazil-s-lgpd-takes-effect-are-you-ready [https://perma.cc/KAA8-4C63].

[88] Lei No. 13,709, de 14 Agosto de 2018, Diário Oficial Da União [D.O.U.] (1), (5, t.1) (Braz.).

[89] *Id.* § 12.

[90] *Id.* § 9.

[91] *Id.* art. 5, 7, 8.

[92] *Id.* art. 8(5).

a right of access to their collected personal data[93] and the right to correct or delete such collected personal data[94]—effectively a right to be forgotten similar to those in the GDPR and PPDA. Also similarly to the GDPR and the PDPA, for the international transfer of data, the LGPD requires an adequate level of protection in the recipient country or another form of guarantee, such as the data subject's specific consent.[95]

4. Canada

[20] Canada, like the United States, as discussed below in Part III, governs data protection through a patchwork of federal, provincial, and territorial legislation.[96] However, unlike the United States, Canada has a comprehensive federal level law.[97] Canada's federal consumer data protection law is the Personal Information Protection and Electronic Documents Act ("PIPEDA").[98] The PIPEDA applies to all organizations that collect, use, or disclose personal information in the course of commercial activities and information that is collected about an employee or applicant.[99] It does not apply to government organizations, which are covered by the Privacy Act instead, and the Governor in Council may forbear from applying the PIPEDA in provinces where there is "substantially similar" legislation (so far determined to be the case in

[93] *Id.* art. 9, 18.

[94] *Id.* art. 18(3), (6).

[95] *Id.* art. 33(1).

[96] DLA PIPER, *supra* note 60.

[97] *PIPEDA Legislation and Related Regulations*, OFF. OF THE PRIV. COMM'R OF CAN., (Jan. 9, 2018), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/ [https://perma.cc/4636-WXJZ].

[98] Personal Information Protection and Electronic Documents Act, S.C. 2000 c. 5 (Can.).

[99] *Id.*

Alberta, British Columbia, and Quebec).[100] The PIPEDA protects personal information, defined as information about an identifiable person,[101] but does not address whether anonymous or pseudonymous data would qualifyunder this definition.[102]

[21] The PIPEDA requires data collectors to identify the purpose for collection[103] and obtain the informed consent of the data subject before collection can start.[104] There is not an explicit opt-out right for the sale of personal information, but consent may be withdrawn at any time.[105] A data subject may access their collected personal data, but unlike the GDPR, PPDA, and LGPD, the data subject cannot change the data collected about them unilaterally, but must first prove the collected data's inaccuracy.[106] Unlike the GDPR, PPDA, and LGPD, there is also no right to delete one's collected personal information unless it is proven to be inaccurate.[107] Also unlike the GDPR, PPDA, and LGPD, PIPEDA does not have restrictions

[100] *Id.* at art. 26(2)(b); *see also* DLA PIPER, *supra* note 60, at 116 (listing the provinces where PIPEDA and its iterations apply).

[101] *See* Personal Information Protection and Electronic Documents Act, S.C. 2000 c. 5, art. 2(1), 3 (Can.) (highlighting the purpose and scope of the Act).

[102] *See id.* at art. 2(1) (showing that the definition of personal information does not include the terms anonymous or pseudonymous).

[103] *Id.* sched. 1, art. 4.2.

[104] See *id.* at art. 6.1 (demonstrating that consent is valid only when the individual is informed); *see also id.* sched. 1, art. 4.3.

[105] Personal Information Protection and Electronic Documents Act, S.C. 2000 c. 5, sched. 1, art. 4.3.8.

[106] *See id.* sched. 1, art. 4.9 (stating that although an individual may access her personal data, she may not alter the data without first challenging its accuracy).

[107] *See id.* sched. 1, art. 4.9.5 (stating that, depending on the nature of the information, the organization will amend the information; however, the process does not ensure the information's deletion).

on the international transfer of personal data based on adequacy determinations.[108]

5. Israel

[22] Data privacy in Israel is primarily regulated by the Protection of Privacy Law and its regulations ("PPL").[109] The law protects "data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person."[110] The law does not directly address anonymous, deidentified, pseudonymous, or aggregated data.[111]

[23] Israel requires data collectors to register their databases with the state of Israel for a particular purpose.[112] Data subjects must consent to this purpose, although consent may be implied as well as explicit, unlike the GDPR, PPDA, LGPD, and PIPEDA.[113] The PPL does not provide a right to withdraw consent or opt out of the sale of personal information.[114] However, data subjects do have the right to inspect any information kept

[108] *See* Timothy M. Banks, *How did Canada Fare on Privacy in the USCMA?*, IAPP (Oct. 12, 2018), https://iapp.org/news/a/how-did-canada-fare-on-privacy-in-the-usmca [https://perma.cc/B392-DPFG].

[109] DLA Piper, *supra* note 60, at 369; Protection of Privacy Law, 5741-1981, (1981) (as amended) (Isr.); Protection of Privacy Regulations, 5777-2017, (2017) (as amended) (Isr.).

[110] Protection of Privacy Law, 5741-1981, § 7 (1981) (as amended) (Isr.).

[111] *See id.* at §§ 3, 7.

[112] *See* Protection of Privacy Regulations, 5777-2017, § 2(a)(2), (2017) (as amended) (Isr.); *See also* Protection of Privacy Law, 5741-1981, § 8(a)(2), (1981) (as amended) (Isr.).

[113] *See* Protection of Privacy Law, 5741-1981, §§ 1, 3, (1981) (as amended) (Isr.); *See also* DLA Piper, *supra* note 60, at 370.

[114] *See* Protection of Privacy Law, 5741-1981, §§ 1, 3, (1981) (as amended) (Isr.).

on them in a database.[115] Data subjects may also request corrections to any incorrect information, although the data collector is not obligated to correct such information unless they agree that it is incorrect or are compelled to do so by a court order.[116] Unlike the GDPR, PPDA, and LGPD, but like the PIPEDA, the PPL provides no right to delete one's collected personal information.[117] Israel has a standard for cross-border data transfer similar to the GDPR, PDPA, and LGPD, requiring that the recipient country "ensures a level of protection no lesser, *mutatis mutandis*, than the level of protection of data provided for by IsraeliLaw,"[118] although the data subject may also consent notwithstanding the recipient country's regulations.[119]

6. Japan

[24] The Act on the Protection of Personal Information ("APPI") codifies Japan's national data protection law.[120] The APPI regulates the use of personal information, defined as information about a living individual which can identify the specific individual by name, date of birth, or other description contained in such information.[121] The APPI does not refer to anonymized or pseudonymized data, but personal information

[115] *Id.* at § 13(a)–(b).

[116] *Id.* at § 14.

[117] *See id.* at §§ 12–15.

[118] Protection of Privacy (Transfer of Data to Databases Abroad) Regulations, 5761-2001, § 1 (2001) (Isr.).

[119] *See id.* at § 2.

[120] *See* Act on the Protection of Personal Information, No. 57 (2003) (Japan); *see also* Tomoki Ishiara, *Japan*, *in* PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 220, 220 (Alan Charles Raul ed., 5th ed. 2018).

[121] Act on the Protection of Personal Information, art. 2 (1) (Japan).

does include "individual identification codes," or unique numbers assigned to a data subject.[122]

[25] The APPI requires data collectors to specify the purpose of collection as much as possible,[123] including notifying data subjects of this purpose.[124] Unlike the GDPR, LGPD, or PPL, the APPI only requires consent to the extent that a use of the data goes beyond this specified purpose,[125] although consent is generally required for transfer to a third party.[126] The APPI does not refer to the sale of information or a right to withdraw consent.[127] Upon the data subject's request, the data collector must disclose what personal information they have collected on that particular data subject.[128] If the data subject requests that the collected information be amended or deleted due to being incorrect, a data collector must investigate and take action in conformity with its findings,[129] which places an emphasis on truth similar to the PPL rather than on the right to be forgotten like under the GDPR, PPDA, and LGPD. Consistent with the GDPR, PDPA, LGPD, and PPL, for international transfers of data, the APPI requires the data subject's consent, certain emergency circumstances, or that the data is sent to "foreign countries possessing

[122] *Id.* at art. 2(1)(ii).

[123] *See id.* at art. 15(1).

[124] *See id.* at art. 18(1).

[125] *See id.* at art. 16(1).

[126] *See id.* at art. 23(1).

[127] *See Online Privacy Law: Japan,* LIBRARY OF CONGRESS (2012), https://www.loc.gov/law/help/online-privacy-law/2017/japan.php. [https://perma.cc/RU3Z-24AC].

[128] *See* Act on the Protection of Personal Information, art. 28 (Japan).

[129] *See id.* at art. 29.

personal information protection systems recognized to be at the same level as Japan's in terms of protecting the rights and interests of individuals."[130]

7. New Zealand

[26] New Zealand's privacy law is governed by the Privacy Act 2020, which took effect on December 1, 2020.[131] The Privacy Act covers personal information, defined as information about an identifiableindividual.[132] The Privacy Act does not explicitly address anonymization and pseudonymization, and it allows unique identifiers as long as certain procedures are followed.[133]

[27] The Privacy Act requires that data collectors take reasonable steps to make data subjects aware of, *inter alia*, the collection of their personal data, the purpose of that collection, the intended recipient of that data, and the rights of access to, and correction of, the information provided by the collector.[134] The Privacy Act states that prior to collecting personal data, the consent of the data subject should be acquired, where appropriate.[135] However, there is no mention in the Privacy Act of an explicit opt out or withdrawal of consent right.[136] Data subjects must have access to the personal information that has been collected on them, if requested.[137] Like

[130] *Id.* at art. 23–24.

[131] Privacy Act 2020, Privacy Commissioner, https://www.privacy.org.nz/privacy-act-2020/privacy-act-2020 [https://perma.cc/PDL2-U8SW].

[132] *See* Privacy Act 2020, pt. 1, s 7 (N.Z.).

[133] *See id.* at pt. 3, s 22, princ. 13.

[134] *See id.* at pt. 3, s 22, princ. 3

[135] *Id.* at sch 8.

[136] *See id.* at sch 8.

[137] *Id.* at pt. 3, s 22, princ. 6.

the APPI, the Privacy Act allows data subjects to request the correction of their personal data, and the data collector must investigate whether the personal information at issue is indeed correct,[138] although no deletion right is mentioned.[139] Under the Privacy Act, the Privacy Commissioner may issue a transfer prohibition notice, which prohibits the transfer of personal information to a specified country "where it will not be subject to a law providing comparable safeguards to this Act."[140] This is similar to the prerequisite of adequately equivalent levels of data protection for international data transfers under the GDPR, PPDA, LGPD, PPL, and APPI. The standard is reversed, however, since all countries are presumed acceptable until they are deemed unacceptable by the Privacy Commissioner;[141] under the above laws, the presumption is that no other country is acceptable until individually authorized by the home state.

8. Switzerland

[28] Data privacy in Switzerland is regulated by the Federal Act on Data Protection ("FADP"),[142] which was recently revised to be more in line with the GDPR.[143] The FADP protects individuals' personal data, defined as "all information relating to an identified or identifiable

[138] *Id.* at pt. 3, s 22, princ. 7.

[139] *See id.*

[140] *Id.* at pt. 8, s 193.

[141] *Id.*

[142] Bundesgesetz über den Datenschutz [DSG] [Federal Act on Data Protection], June 19, 1992 (as amended Mar. 1, 2019) (Switz.); DLA PIPER, *supra* note 60, at 721.

[143] Grégoire Uldry & Olivier Cavadini, *The General Data Protection Regulation (GDPR) and the Revised Swiss Data Protection Act (DPA) - Advice for Trustees based in Switzerland*, CHARLES RUSSELL SPEECHLYS INSIGHTS, https://www.charlesrussellspeechlys.com/en/news-and-insights/insights/private-client/2018/the-general-data-protection-regulation-gdpr-and-the-revised-swiss-data-protection-act-dpa/ [https://perma.cc/F6K4-RPUH].

person."[144] The FADP does not refer to anonymized, deidentified, pseudonymous, or aggregated personal data.[145]

[29] The FADP effectively contains a notice requirement, as personal data may only be processed for the purpose that is given at the time of collection.[146] If consent is required to process the personal data, the consent must be informed, but the FADP only explicitly requires consent when processing sensitive personal data,[147] which is more limited than the GDPR, PDPA, LGPD, PPL, and APPI.[148] There is also no explicit right toopt-out of sales or withdraw consent.[149] However, data collectors must

[144] Bundesgesetz über den Datenschutz [DSG] [Federal Act on Data Protection], June 19, 1992 (as amended Mar. 1, 2019), art. 2-3 (Switz.).

[145] *See id.*

[146] *See id.* at art. 4(3).

[147] *See id.* at art. 4(5).

[148] *See What are the GDPR Consent Requirements?*, GDPR.EU, https://gdpr.eu/gdpr-consent-requirements/ [https://perma.cc/7F59-VNE2]; *see also* Tay & Partners, *Practical Guidance on Compliance with the Personal Data Protection Act 2010 ("PDPA"),* LEXOLOGY.COM, (Dec. 9, 2019), https://www.lexology.com/library/detail.aspx?g=816a2a78-0515-4e21-990c-020d0d608f4d [https://perma.cc/DXJ5-RSYW]; *Comparing Privacy Laws: GDPR v. LGPD* 22*,* DATAGUIDANCE.COM, http://www.dataguidance.com/sites/default/files/gdpr_v_lgpd_revised_edition.pdf [https://perma.cc/EU58-GW4Y]; *Online Privacy Law: Israel,* LAW LIBRARY OF CONGRESS, https://www.loc.gov/law/help/online-privacy-law/2012/israel/php [https://perma.cc/JC6Y-CHZ5]; Hiromi Hayashi & Masaki Yukawa, *Japan: Data Protection Laws and Regulations 2020,* ICLG.COM, (June 7, 2020), https://iclg.com/practice-areas/data-protection-laws-and-regulations/japan [https://perma.cc/5FQV-HC5S].

[149] *See Data Protection Information* 3*,* ROTHSCHILD & CO WEALTH MANAGEMENT, https://www.rothschildandco.com/siteassets/publications/rothschild/private_wealth/legal/en-zurich-data-protection-information.pdf [https://perma.cc/Z9NN-U7S4]; *see also* Bundesgesetz über den Datenschutz [DSG] [Federal Act on Data Protection], June 19, 1992 (as amended Mar. 1, 2019), art. 2–3 (Switz.).

provide access to all data concerning a data subject upon request.[150] Data subjects may request that any incorrect data about them be corrected,[151] but the process is not described in the FADP and no right to be forgotten is mentioned.[152] Similarly to the GDPR, PPDA, LGPD, PPL, APPI, and Privacy Act, for personal data to be transferred internationally, there must be legislation in the recipient country that "guarantees adequate protection," or there must be an exception, such as the data subject's specific consent.[153]

9. Uruguay

[30] Uruguay's data protection law is governed by the Act on the Protection of Personal Data and Habeas Data Action ("Data Protection Act").[154] The Data Protection Act applies to personal data, defined as information of any kind related to an identifiable person, in any format that makes processing possible.[155] Dissociated data is subject to more limited regulations.[156]

[150] *See id.* art. 8(1)

[151] *See id.* art. 5(2).

[152] *See What does the Revision of the Swiss Data Protection Act Entail, and How Does It Relate to the GDPR and the ePrivacy Regulation?,* PRICEWATERHOUSE COOPERS, 6, https://www.pwc.ch/en/publications/2018/e-dsg-pov.pdf [https://perma.cc/R98J-DT5].

[153] Federal Act on Data Protection, art. 6.

[154] Protección de Datos Personales y Acción de "Habeas Data" [Act on the Protection of Personal Data and Habeas Data Action], Law No. 18,331, Aug. 18, 2008 (as amended) (Uru.); DLA PIPER, *supra* note 60, at 851.

[155] Act on the Protection of Personal Data and Habeas Data Action, art. 3, 4(D).

[156] *Id.* at art. 17(D).

[31] Data subjects must be notified in an express, unequivocal, and clear way of the purpose for which their collected data will be used.[157] Processing of personal data generally requires the express informed consent of the data subject, consistent with the GDPR, PPDA, LGPD, PIPEDA, and FADP.[158] The data subject may block his data from being used for advertising and sales purposes.[159] Under the Data Protection Act, data subjects have a right of access to their collected data, albeit they may only exercise this right once every six months.[160] Data subjects also have the right to request the correction or deletion of their personal data, subjectto limited restrictions,[161] providing a right to be forgotten like the GDPR, PPDA, and LGPD. Data may only be transferred to third parties if authorized by law or with the informed consent of the data subject,[162] but personal data may not be transferred internationally unless the recipient country provides adequate levels of data protection,[163] which is similar to the GDPR, PPDA, LGPD, PPL, APPI, Privacy Act, and FADP.

[157] *Id.* at art. 13.

[158] *Id.* at art. 9.

[159] *Id.* at art. 21.

[160] *Id.* at art. 14.

[161] *Id.* at art. 15.

[162] *Id.* at art. 8.

[163] *Id.* at art. 23.

Table 1: Comparison of Foreign Data Law Rights and Obligations

	Notice	Consent	Opt- Out of Sales / Withdrawal Right	Access	Correction	Deletion	Adequacy Requirement for International Transfer
EU	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Argentina	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Brazil	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Canada	Yes	Yes	Yes	Yes	Yes	No	No
Israel	(to state)	(implied or explicit)	No	Yes	Yes	No	Yes
Japan	Yes	(only if for a different purpose)	No	Yes	Yes	No	Yes
New Zealand	(reasonable steps)	Yes	No	Yes	Yes	No	Yes
Switzerland	Yes	(only for sensitive personal data)	No	Yes	Yes	No	Yes
Uruguay	Yes	Yes	Yes	Yes	Yes	Yes	Yes

III. U.S. DATA PRIVACY LAW

[32] Data protection law in the United States stands in contrast to the nine foreign laws discussed in Part II(B). U.S. data protection law is not codified in a single primary national regulation,[164] nor does it cover several of the rights and obligations contained in those previous nine national laws,[165] although certain states do have regulations approaching those laws' breadth.[166]

A. Federal Data Protection Law

[33] First, instead of a comprehensive data protection law like many other countries, the United States instead has a patchwork of federal and state laws governing data protection practices.[167] Most federal data protection laws focus on a single industry, such as financial institutions (theGramm-Leach-Bliley Act, "GLBA,"[168] and the Consumer Financial Protection Act, "CFPA"),[169] health care entities (the Health Insurance Portability and Accountability Act, "HIPAA"),[170] and communications

[164] Steven Chabinsky & F. Paul Pittman, *Relevant Legislation and Competent Authorities, in* DATA PROTECTION 2020 417 (7th ed, 2020) https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa#:~:text=There%20is%20no%20single%20principal%20data%20protection%20legislation%20in%20the%20United%20States.&text=broadly%20empowers%20the%20U.S.%20Federal,privacy%20and%20data%20protection%20regulations [https://perma.cc/MR47-GRYT].

[165] *See id.*

[166] *See id.*

[167] *See* MULLIGAN ET AL., *supra* note 16, at 7, 36.

[168] *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 103, 113 Stat. 1338, 1342-1351 (1999).

[169] 12. U.S.C. § 5481. (2010).

[170] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (1996).

common carriers (the Communications Act of 1934, as amended by the Telecommunications Act of 1996),[171] or specific types of data, such as data related to consumers' creditworthiness (the Fair Credit Reporting Act, "FCRA")[172] or children's data (the Children's Online Privacy Protection Act, "COPPA").[173] On top of this, each of the fifty states has its own laws on data privacy, including privacy causes of action under common law tort and contract claims and data breach response laws, as well as their own statutory frameworks for data protection.[174]

[34] At present, the primary federal vehicle for protecting U.S. consumers' data is the Federal Trade Commission ("FTC") Act.[175] However, the FTC's authority is not rooted in specific data protection law.[176] Instead, the FTC is given broad authority to prevent "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[177] Importantly, this includes any act or practice which "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[178] The FTC's authority has been used to reign in some of the

[171] *See* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 57 (codified as amended at 47 U.S.C. § 151).

[172] *See* Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1128 (1970) (codified as amended at 15 U.S.C. § 1681).

[173] *See* Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681–728 (codified as amended at 15 U.S.C. § 6501).

[174] *See* MULLIGAN ET AL., CONG. RES. SERV., *supra* note 16, at 36–37.

[175] *See id*. at 30.

[176] *About the FTC*, FTC.GOV, https://www.ftc.gov/about-ftc [https://perma.cc/K23U-MHVE].

[177] 15 U.S.C. § 45(a)(1) (2018).

[178] *Id.* at § 45(n).

most egregious privacy practices, effectively creating a common law equivalent for privacy policies.[179] Notably, the FTC recently required one large social media company to pay a $5 billion penalty in 2019.[180] Despite this potentially powerful restriction, however, the FTC has primarily only acted when a data collector fails to disclose in advance that it will be invading a person's privacy.[181] Once such notice is given, the argument for deceptive trade practices which would place data collectors under the FTC's jurisdiction quickly evaporates, creating a significant barrier to comprehensive consumer data protection.[182]

[35] While the FTC may be the closest thing to comprehensive federal data privacy legislation in the United States,[183] it falls short of achieving the same rights as the nine foreign laws from Part II(B).[184] The FTC has said that it protects personally identifiable information, and has broadened this definition to include cases "when [the data] can be reasonably linkedto a particular person, computer, or device," and it has excluded anonymized

[179] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law*, 114 COLUM. L. REV. 583 (2014).

[180] *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/7LXS-LWPH].

[181] FED. TRADE COMM'N., Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers ii (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/Y6FW-GNK7].

[182] *See* Andrews, *supra* note 11, at 449.

[183] Solove & Hartzog, *supra* note 179, at 586–87.

[184] *Compare id., with supra* Part II(B).

data from this definition.[185] This is basically consistent with the foreign data privacy laws from Part II(B).[186] The more problematic comparison is in the substantive requirements and obligations for data collectors. The FTC has required that proper notice of data collection and processing practices be given to consumers,[187] but this is a standard that is followed on a case-by-case basis *ex post* rather than as an *ex ante* rule like with the GDPR and the other eight laws in Part II(B).[188] The FTC has also held data collectors responsible for not collecting consent prior to collection, but again this is *ex post* common law enforcement rather than a specific rule.[189] Indeed, this shortcoming was one impetus for the proposed Customer Online Notification for Stopping Edge-Provider Network Transgressions ("CONSENT") Act[190], which would have required a specific opt-in to data collection akin to that of the GDPR.[191] While certain acts do require the right to opt-out

[185] Jessica Rich, *Keeping Up with the Online Advertising Industry*, FED. TRADE COMM'N (Apr. 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry [https://perma.cc/8TMF-7QJD].

[186] *Compare id., with supra* Part II(B).

[187] *See* Solove & Hartzog, *supra* note 179, at 634.

[188] *See, e.g.*, Complaint at 7–9, In re Facebook, Inc., F.T.C. File No. C-4365 (F.T.C. July 27, 2012); Complaint at 1–2, In re Sears Holdings Mgmt. Corp., F.T.C. File No. C-4264 (F.T.C. Aug. 31, 2009).

[189] *See, e.g.*, Agreement Containing Consent Order at 4, In re Goldenshores Techs., LLC, No. 132-3087 (F.T.C. Dec. 5, 2013); F.T.C. v. Accusearch, Inc., No. 06-CV-0105, 2007 WL 4356786, at *6 (D. Wyo. Sept. 28, 2007).

[190] *See* Alyson Sandler, *Senate Democrats Propose CONSENT Act*, COVINGTON: INSIDE PRIVACY (Apr. 12, 2018), https://www.insideprivacy.com/united-states/congress/senate-democrats-propose-consent-act [https://perma.cc/H6WG-YQ8U].

[191] Customer Online Notification for Stopping Edge-Provider Network Transgressions Act, S. 2639, 115th Cong. § 2(b)(2)(B)(iii) (2018).

from marketing,[192] there is no explicit right to withdraw consent.[193] There is also no required opt-out right for the sale of one's collected personal data, and as long as it is included in the initial disclosure to the data subject, there would not be grounds for an FTC investigation under deceptive trade practices.[194] Perhaps the greatest concern is that there are currently no rights to access, correct, or delete personal information, giving U.S. consumers little control over their data.[195] There are also no federal level restrictions on the cross-border transfer of personal data, with the exception of some government information.[196]

[36] Other federal laws provide some of these rights.[197] Some laws relating specific types of data have expressly required notice and consent for personal data collection, such as COPPA for children under theage of thirteen.[198] There are also rights of access to data in other laws, suchas

[192] *See* Steven Chabinsky & F. Paul Pittman, *USA: Data Protection 2019*, ICLG (June 7, 2020), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa [https://perma.cc/G777-YRME].

[193] Katarina Rebello, *Does the U.S. Need an American Alternative to the GDPR,* THE TRANSATLANTIC PUZZLE (Sept. 19, 2019), https://transatlanticpuzzle.com/ 2019/09/19/ does-the-u-s-need-an-american-alternative-to-the-gdpr/ [https://perma.cc/T385-MD7N].

[194] *See* Andy Green, *Complete Guide to Privacy Laws in the US*, VARONIS (Mar. 29, 2020), https://www.varonis.com/blog/us-privacy-laws/ [https://perma.cc/3JSL-3ZRC].

[195] *See* Yaki Faitelson, *Why "Right to Delete" Should Be on Your IT Agenda Now*, FORBES (Oct. 22, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/ 10/22/why-right-to-delete-should-be-on-your-it-agenda-now/#26ba01fc1b7f [https://perma.cc/D6QW-XBJV].

[196] DLA PIPER, *supra* note 60, at 801.

[197] *See, e.g.*, Children's Online Privacy Protection Act, 15 U.S.C.S. § 6502 (LEXIS through Pub. L. No. 116-163) (regulating the collection of personal information from minors); 45 C.F.R. § 164.306 (2013) (establishing national data security standards for health information).

[198] *See* 15 U.S.C. § 6502(b)(1)(A) (2018).

HIPAA, but no right to be forgotten.[199] Overall, however, the lack of explicit rights to notice, consent, access, correction, and deletion has led groups to clamor for a federal data protection law.[200] Indeed, scholars, politicians, and even the FTC itself, have called for comprehensive federal data protection legislation.[201] The Trump Administration criticized a comprehensive federal data protection law, rejecting the adoption of a prescriptive model like that of the GDPR.[202] While hopes for a comprehensive federal data protection law in the United States were unfulfilled under the Trump Administration, the Biden Administration is expected to consider such a law much more favorably.[203]

[199] *See* Lothar Determann, *Healthy Data Protection*, 26 MICH. TECH. L. REV. 229, 242 (2020).

[200] *See, e.g.*, SOFTWARE & INFORMATION INDUSTRY ASSOCIATION'S RESPONSE TO THE FEDERAL TRADE COMMISSION'S REQUEST FOR COMMENTS ON QUESTIONS IN CONNECTION WITH ITS FEBRUARY 2019 PRIVACY HEARING at 6–7 (Dec. 21, 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/12/ftc-2018-0098-d-0017-163225.pdf [https://perma.cc/D6Q5-CPLT].

[201] *See, e.g.*, Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*, 10 CYBARIS, INTELL. PROP. L. REV. 1, 40 (2019); Alexis Collins et al., *FTC Commissioners Continue Calls for National Data Privacy and Security Legislation*, CLEARY CYBERSECURITY & PRIVACY WATCH (May 29, 2019), https://www.clearycyberwatch.com/2019/05/ftc-commissioners-continue-calls-for-national-data-privacy-and-security-legislation [https://perma.cc/NRM3-XG4F]; Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS INST. (Jul. 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game [https://perma.cc/C39W-JZFX].

[202] *See* MULLIGAN ET AL., *supra* note 16, at 51–52.

[203] Kristin L. Bryan et al., *Election 2020: Looking Forward to What a Biden Presidency May Mean for Data Privacy and Data Privacy Litigation*, NAT'L L. REV. (Nov. 12, 2020), https://www.natlawreview.com/article/election-2020-looking-forward-to-what-biden-presidency-may-mean-data-privacy-and [https://perma.cc/Q286-G8MW].

B. The California Consumer Privacy Act

[37] The California Consumer Privacy Act ("CCPA") is currently by far the most comprehensive state-level data privacy act effective in the United States.[204] However, a growing number of states are starting to consider, or have already passed, legislation on consumer data protection.[205] The CCPA, and this growing body of other state laws, comes much closer to matching the scope of protections of the GDPR, PPDA, LGPD, PIPEDA, PPL, APPI, Privacy Act, FADP, and Data Protection Act than the FTC.[206]

[38] The CCPA explicitly protects personal information, with the statute even providing a list of specific categories of personal information.[207] It explicitly exempts deidentified or aggregated data from the ambit of personal information.[208] Consumers must be informed about what personal information is collected and the purpose for the collection.[209] However, the CCPA does not require consent except for children under the age of sixteen,[210] effectively making it the weakest consent requirement compared to the nine laws examined above in Part II(B).[211] Yet the CCPA goes further than the GDPR, and even further than the PPDA, LGPD, PIPEDA,

[204] *See* Andy Green, *Complete Guide to Privacy Laws in the US*, VARONIS (Mar. 29, 2020), https://www.varonis.com/blog/us-privacy-laws [https://perma.cc/S38E-LSJS].

[205] *See* Sarah Rippy, *US State Comprehensive Privacy Law Comparison*, IAPP (Oct. 14, 2020), https://iapp.org/resources/article/state-comparison-table/ [https://perma.cc/LU3S-F7JA].

[206] *See* Jehl & Friel, *supra* note 61.

[207] *See* CAL. CIV. CODE §§ 1798.140(o), 1798.145(c)–(f) (West 2020).

[208] *See* CAL. CIV. CODE § 1798.145(a)(5) (West 2020); *see also* CAL. CIV. CODE §§ 1798.140(a), (h), (o), (r), (West 2020).

[209] CAL. CIV. CODE § 1798.100(a)–(b) (West 2020).

[210] *See* CAL. CIV. CODE § 1798.120(c)–(d) (West 2020).

[211] *See supra* Part II(B).

and the Data Protection Act, in requiring a "do not sell my personal information" link on the website homepage.[212] Consumers have the right to access their personal data[213] and delete it,[214] although there is no right under the CCPA to correct one's personal information.[215] But, similarly to the PIPEDA, the CCPA has no explicit restrictions on the transfer of data outside of California,[216] such as the adequacy requirements required under the GDPR, PPDA, LGPD, PPL, APPI, Privacy Act, FADP, and Data Protection Act.[217]

[39] The CCPA clearly comes much closer to leading foreign data privacy regimes than the U.S. federal patchwork, but its greatest downside is that it only protects the data of California residents, not the U.S. population at large.[218] Therefore, the CCPA can not serve as a substitute for comprehensive U.S. federal data privacy legislation, except for Californians. Indeed, the CCPA serves as an example of thegeographic patchwork of data privacy inequality in the United States, where citizens of some states are protected while citizens of otherstates have woefully insufficient rights.[219]

[212] *See* CAL. CIV. CODE §§ 1798.135(a)–(b) (West 2020).

[213] *See* CAL. CIV. CODE §§ 1798.100(d), 1798.110, 1798.115 (West 2020).

[214] CAL. CIV. CODE § 1798.105 (West 2020).

[215] *See* Jehl & Friel, *supra* note 61, at 5.

[216] *See* CAL. CIV. CODE §§ 1798.115, 1798.130, 1798.135 (West 2020).

[217] *See, e.g.*, GENERAL DATA PROTECTION REGULATION (GDPR), art. 44 (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [https://perma.cc/XT24-T5SB].

[218] *See* CAL. CIV. CODE § 1798.140(g) (West 2020).

[219] *See* Goodyear, *supra* note 5, at 89.

IV. PENUMBRAS OF DATA PRIVACY IN OTHER COUNTRIES

[40] Given the lack of comprehensive federal data protection legislation in the United States and the stark disparity between different states' consumer data protection laws, U.S. consumers are faced with significant dangers from the use, or rather misuse, of their personal information.[220] But U.S. consumers are better protected due to influence from an unlikely source: foreign data protection laws. It is true that all of the national data protection laws discussed in Part II(B) only protect their own nationals.[221] Therefore, U.S. citizens of course do not benefit directly from these stronger foreign data privacy protections; but there can be (potentially quite significant) spillover effects.[222] Stronger foreign dataprotection regimes cast penumbras onto data privacy in the United States through foreign regulations applying to U.S. entities,[223] increased global awareness of data privacy issues,[224] increased adoption of robustdata protection laws,[225] and serving as direct examples for adoption by other jurisdictions.[226]

[220] *See, e.g.*, Andrews, *supra* note 11, at 428–43 (discussing the misuse of personal data by mobile medical apps). *See generally* Andy Smith, *The Dangers of Data Collection*, BCS (June 26, 2019) (detailing the use of data mining to target individuals).

[221] *See* Dan Storbaek, *A Complete Guide to GDPR, CCPA and International Privacy Laws*, SECURE PRIVACY (Aug. 31, 2018), https://secureprivacy.ai/complete-guide-to-international-data-privacy-laws [https://perma.cc/YXT2-3DHR].

[222] *See* Lindsey O'Donnell, *What Will GDPR's Impact Be On U.S. Consumer Privacy?*, THREATPOST (May 24, 2018 3:29 PM), https://threatpost.com/what-will-gdprs-impact-be-on-u-s-consumer-privacy/132137 [https://perma.cc/Q2NP-X3KM].

[223] *See infra* Part IV(A).

[224] *See infra* Part IV(B).

[225] *See infra* Part IV(C).

[226] *See infra* Part IV(D).

A. Regulation of U.S. Entities

[41] Foreign data protection laws directly regulate the actions of many U.S. entities.[227] The GDPR, LGPD, and other foreign data privacy laws apply to organizations established outside their jurisdiction if the organizations process the personal data of data subjects inside their jurisdiction.[228] So U.S. companies that operate in these jurisdictions are forced to comply with these foreign data protection laws if they wish to continue operating there.[229] Therefore, due to the national level regulation of data privacy, global companies are effectively left with two choices: adopt different standards for each jurisdiction or adopt a one-size-fits-all policy.[230]

[42] While U.S. companies go both ways, there is substantial economic and technical pressure for these companies to follow the most stringent standard.[231] Experts conclude that it is far easier to have the same privacy rules globally than adopt piecemeal practices for each jurisdiction.[232] According to Massachusetts Institute of Technology professor Sinan Aral,

> [I]t is not efficient and in fact potentially not even possible to segregate consumers that are in Europe or sometimes in Europe, and then consumers that are outside of Europe . . . A large fraction of the changes that are going to be required

[227] *See* Neema Singh Guliani & Jay Stanley, *The Landmark European Law That Could Change Facebook and Improve Privacy in America*, ACLU (Apr. 12, 2018), https://www.aclu.org/blog/privacy-technology/internet-privacy/landmark-european-law-could-change-facebook-and-improve [https://perma.cc/7RNF-HSPP].

[228] *See, e.g.*, Council Regulation 2016/679, art. 3, 2016 O.J. (L 119) 59; Lei No. 13.709, de 14 Agosto de 2018, DÍARIO OFICIAL DA UNIÃO [D.O.U] art. 3 de 15.8.2018 (Braz.).

[229] *See* Guliani & Stanley, *supra* note 227.

[230] *See id.*

[231] *See id.*

[232] *See* O'Donnell, *supra* note 222.

> of these companies to become compliant will need to apply to everyone.[233]

Consumer rights group Consumer Action echoed Professor Aral's opinion, concluding that it is unlikely that large global corporations will create country-specific systems for data protection and maintenance practices.[234]

[43] Due to this reality, many U.S. companies have already developed new data protection practices to comply with the GDPR.[235]Some of these companies have stated that they will apply their GDPR- compliant data protection practices on a company-wide basis rather than just while operating in the EU.[236] For example, major data collecting companies such as Microsoft and Facebook said they would apply GDPR protections to all of their customers, not just in Europe.[237] This is especially the case because, at least with the GDPR, companies have to consider not only whether they collect data directly from European consumers, but also whether they do business with a company that operates in the EU.[238] According to a recent study polling 194 U.S. firms, many firms revised their privacy policies to comply with a least some of the major GDPR provisions, even when their contracts

[233] *Will the EU's GDPR Rules Launch a New Era of Data Protection?*, WHARTON U. PA.: KNOWLEDGE@WHARTON (May 24, 2018), https://knowledge.wharton.upenn.edu/article/how-the-gdpr-rules-will-impact-data-protection [https://perma.cc/6GQW-4G6Q].

[234] Warwick Ashford, *GDPR Will Have Positive Ripple Effect, Says US Consumer Group*, COMPUTERWEEKLY.COM (Feb. 27, 2018), https://computerweekly.com/news/252435774/GDPR-will-have-positive-ripple-effect-say-US-consumer-group [https://perma.cc/AB85-3YGB].

[235] *See* MULLIGAN ET AL., *supra* note 16, at 50.

[236] *See id.*

[237] O'Donnell, *supra* note 222.

[238] Guliani & Stanley, *supra* note 227.

aimed at U.S. rather than European consumers.[239] These revisions led to significant increases in personal data rights of users from 2014 to 2018, such as the ability to access and correct personal data and the destruction or anonymization of personal data upon account termination.[240]

[44] Therefore U.S. consumers have benefitted directly from the spillover effects of stricter foreign data privacy laws. This trend will grow as stricter data privacy laws expand globally.[241] While the GDPR has garnered an enormous amount of press, newly emerging data privacy laws, such as those of Brazil and Thailand, both of which went into effect in 2020,[242] will place more of the world's Internet users under the jurisdiction of GDPR-esque regulations. This, in turn, increases the economic pressure on U.S. companies to create a one-size-fits-all model as they have to adopt these practices in an increasingly large number of countries. The same is true on the national scale; the CCPA, and future consumer data privacy laws in other states, make it even harder for U.S. companies to maintain disparate privacy practices in different jurisdictions, as they would have to carve out different practices at an even more granular level.[243]

---

[239] *See* Kevin E. Davis & Florencia Marotta-Wurgler, *Contracting for Personal Data*, 94 N.Y.U. L. REV. 662, 667–668, 694–695 (2019).

[240] *Id.* at 695–699.

[241] Scott Matteson, *Data Privacy: Top Trends to Watch in 2020*, TECHREPUBLIC (January 29, 2020), https://www.techrepublic.com/article/data-privacy-top-trends-to-watch-in-2020/ [https://perma.cc/87VS-QPQ9].

[242] Fatim Jumabhoy et al., *Thailand: Personal Data Protection Act to Take Effect in May 2020*, MONDAQ (Aug. 5, 2019), https://www.mondaq.com/privacy-protection/833068/personal-data-protection-act-to-take-effect-in-may-2020 [https://perma.cc/U4S7-TBGM]; Lissa M. Thomas, *Brazil's New Privacy Law One Year Away*, NAT'L L. REV. (Aug. 21, 2019), https://www.natlawreview.com/article/brazil-s-new-privacy-law-one-year-away [https://perma.cc/W58V-QA8M].

[243] Laura Hautala, *California's New Privacy Rights Could Be Coming to Your State* Too, CNET (Jan. 3, 2020), https://www.cnet.com/news/californias-new-ccpa-privacy-rights-could-come-to-your-state-too [https://perma.cc/QBP4-WFYA].

B. Increased Global Awareness of Data Privacy Issues

[45] The GDPR and other foreign data protection regimes have additional ancillary spillover effects, as they generate increased discussion around privacy and elevate the importance of privacy for consumers. For example, U.S. consumers are inundated with the now-ubiquitous GDPR pop-ups on websites, not to mention emails and news stories related to the GDPR.[244] Companies and policy makers are also forced to reconsider their data practices as more countries adopt strict data privacy laws.[245]

[46] A Pew Research Center study found that U.S. consumers' fears about privacy have increased precipitously in the past few years.[246] Sixty- two percent of Americans found it impossible to go through daily life without companies collecting their personal data.[247] Eighty-one percent found that they have little control over the data companies collect.[248] Seventy-nine percent were concerned about how their data is used, and eighty-one percent concluded that the potential risks of this collection of their data outweigh the potential benefits.[249] These concerns and public awareness about data privacy in general have been aggravated by notable data leakages, including

[244] *See* Danny Palmer, *Where GDPR Goes Next: How Digital Privacy Is Taking Over the World*, ZDNET (May 21, 2019), https://www.zdnet.com/article/where-gdpr-goes-next-how-digital-privacy-is-taking-over-the-world [https://perma.cc/2NDE-PUL3].

[245] *See* Sue Poremba, *The Future of Data Protection and Other RSA Observations*, DATAGRAIL (Mar. 11, 2019), https://datagrail.io/blog/rsa-and-the-future-of-data-protection [https://perma.cc/64NH-8ENQ].

[246] *See* Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Out of Control Over Their Personal Information*, PEW RES. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/ americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information [https://perma.cc/W62J-SPXX].

[247] *Id.*

[248] *Id.*

[249] *Id.*

the Snowden revelations in 2013, the Equifax data breach in 2017, and the Cambridge Analytica data breach scandal in 2018.[250] Indeed, 2018 saw an increase in the number of privacy complaints in practically every country worldwide.[251]

[47] Today, even in countries with weak data protection requirements, being perceived as a secure provider is important for acquiring customers.[252] Until recently, companies hardly worried about privacy perception; the profits from processing and selling data far outweighed miniscule customer concern about privacy.[253] But now, buoyed by increasing conversations about the importance of privacy globally, what companies do with customers' personal data is of considerable interest to consumers.[254] Due to consumers' increased awareness of privacy issues, companies that comply with more stringent standards such as the GDPR are likely to create an increased level of transparency with their U.S. customerstoo.[255]

C. Increased Adoption of Robust Data Privacy Laws

[48] In addition to their influence on data collectors and consumers, foreign data protection laws also have a significant impact on policy

[250] *See* Kerry, *supra* note 201.

[251] *Privacy Is a Global Issue*, PWC (May 8, 2019), https://www.pwc.com/gx/en/news-room/press-releases/2019/global-privacy-enforcement-tracker.html [https://perma.cc/559R-YYN7].

[252] *See Privacy Laws in Different Countries and How to Comply With Them*, WEBSITE POLICIES (Apr. 06, 2020), https://www.websitepolicies.com/blog/privacy-laws-in-different-countries [https://perma.cc/M2ZZ-VSRW].

[253] Thomas C. Redman & Robert M. Waitman, *Do You Care About Privacy as Much as Your Customers Do?*, HARV. BUS. REV. (Jan. 28, 2020), https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do [https://perma.cc/6U2L-26ND].

[254] *See id.*

[255] *Will the EU's GDPR Rules Launch a New Era of Data Protection?*, *supra* note 233.

makers. These robust and influential data privacy laws encourage the adoption of improved data privacy laws in other countries.[256] This is in part through international pressure.[257] In addition, most of these strict data protection laws have restrictions on which countries can receive personal information from their jurisdiction, encouraging foreign jurisdictions to improve their privacy practices or be left out of the global data market.[258]

[49] First, the EU has substantially influenced the development of other countries' legal institutions.[259] The so-called "Brussels Effect" has affected many areas of law, and, if other jurisdictions have overly permissive or weak legal regimes in an area, the "Brussels Effect" can have a significant impact in creating desirable effects in these countries.[260] But this trend is notlimited to the EU. As Professor Anu Bradford found, such a degree of international legal influence requires that "the jurisdiction must have alarge domestic market, significant regulatory capacity, and the propensity to enforce strict rules over inelastic targets (e.g., consumer markets) as opposed to elastic targets (e.g., capital)."[261] This means that large or economically significant countries, such as Brazil and Japan, are likely to have especially significant influences on other countries' practices.[262] The

[256] *See* Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, *Localization Barriers to Trade: Threat to the Global Innovation Economy*, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION 17, 18 (2013), http://www.itif.org/2013-localization-barriers-to-trade.pdf [https://perma.cc/8JZT-YZY7].

[257] *See Privacy and Human Rights, An International Survey of Privacy Laws and Practice*, GLOBAL INTERNET LIBERTY CAMPAIGN, https://www.gilc.nl/privacy/survey/intro.html [https://perma.cc/73QA-C2NR].

[258] *See* U.N. Human Rights Office of the High Commissioner, *The Right to Privacy in the Digital Age*, https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx [https://perma.cc/4NYU-U2Y4].

[259] *See* Anu Bradford, *The Brussels Effect*, 107 NW. U. LAW. REV. 1 (2012).

[260] *Id.* at 64.

[261] *Id.* at 5.

[262] *See id.* at 11.

"Brussels Effect" has been observed in the development of data privacy laws around the globe, especially in the wake of the implementation of the GDPR.[263] Indeed, the EU has actively encouraged other countries to adopt laws similar to the GDPR.[264]

[50] In addition to this incidental influence, countries have also been directly pressured to adopt stricter data privacy laws through the inclusion of "adequacy" determinations in data protection legislation.[265] These adequacy determinations are ubiquitous in recently enacted data privacy laws. Under the GDPR, the primary path for transferring personal data across borders is if those jurisdictions have been deemed to have an "adequate" level of data protection by the European Commission; if not, they have to go through a separate authorization procedure.[266] The PDPA, LGPD, PPL, APPI, Privacy Act, FADP, and Data Protection Act all effectively have this same requirement.[267] Out of the nine foreign privacy acts[268] examined in Part

[263] *See generally* Rustad & Koenig, *supra* note 19, at 387–411 (discussing how U.S. companies have complied with the GDPR). *See* Schwartz, *supra* note 21, at 783–803. *But see* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1986–87(2013) (arguing that the EU's data privacy laws have a more collaborative approach instead of unilateral influence, but it was published before the enactment of the GDPR and primarily discusses the U.S. context).

[264] *See* Adam Satariano, G.D.P.R*., a New Privacy Law, Makes Europe World's Leading Tech Watchdog,* N.Y. TIMES (May 24, 2018)*,* https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html [https://perma.cc/PT7D-VJF5].

[265] *See Adequacy decisions*, Euro. Comm'n, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents [https://perma.cc/4SP9-WX8C].

[266] *See* Council Regulation 2016/679, 2016 O.J. art. 45 (L 119).

[267] *See* LEY DE PROTECCIÓN DE LOS DATOS PERSONALES, Law No. 25.326, Oct. 4, 2000, art. 12 (Arg.); Lei No. 13,709, de 14 Agosto de 2018, art. 33 (Braz.); Protection of Privacy Regulations, 5761–2001, § 1 (2001) (Isr.); Kojin jōhō no hogo ni kansuru hōritsu, Act No. 57 of 2003, art. 24 (as amended in 2016) (Japan); Privacy Act 1993, s 114D (N.Z.); Bundesgesetz über den Datenschutz [DSG], June 19, 1992 (as amended Mar. 1, 2019), art. 6 (Switz.); Protección de Datos Personales y Acción de "Habeas Data," Law No. 18,331, Aug. 18, 2008 (as amended), art. 23 (Uru.).

II(B), only Canada's PIPEDA lacks an adequacy requirement for the cross-border transfer of data.[269]

[51] While individual companies can usually guarantee certain data privacy practices as an alternative to this requirement, it is a significant burden on companies, and it would be far more straightforward for data collectors if the recipient country enacts adequate data protection laws. The European Commission has not determined that the United States has an adequate data protection regime.[270] Meanwhile countries that adopt GDPR-esque privacy legislation, such as Japan, are granted full adequacy by the European Commission.[271]

---

[268] *See supra* Part II (B).

[269] *See PIPEDA in Brief*, Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/ [https://perma.cc/GZ44-HZ2N].

[270] *See Adequacy Decisions*, EURO. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/Q7TT-XSZ3] (last visited Feb. 1, 2021). Cross-border data transfers from the EU to the United States were previously allowed by entities that complied with the optional EU-U.S. Privacy Shield Framework. However, on July 16, 2020, the Court of Justice of the EU invalidated the EU-U.S. Privacy Shield. Case C-311/18, Data Protection Comm'r v. Facebook, July 16,2020, ECLI:EU:C:2020:559.

[271] *See GDPR Brief: Japan Obtains the First Adequacy Agreement Under the GDPR*, GLOBAL ALLIANCE FOR GENOMICS & HEALTH (Oct. 3, 2019), https://www.ga4gh.org/news/gdpr-brief-japan-obtains-the-first-adequacy-agreement-under-the-gdpr [https://perma.cc/A3LL-648C].

[52] Several countries have adopted stricter data protection laws since the GDPR came into effect, many of them modeled on the GDPR itself.[272] For example, Brazil,[273] Thailand,[274] Chile,[275] and Panama[276] all modeled their data protection laws on the GDPR. Other data protection laws, while not necessarily explicitly modeled on the GDPR, are substantively similar to the GDPR in effect, including those of South Korea[277] and Kenya,[278] as well as California's CCPA.[279] Others, such as Argentina,[280] have simply updated their data privacy laws to meet these new GDPR standards. This trend will only increase as more jurisdictions adopt restrictive cross-border data transfer laws and flex their international influence.

---

[272] *See id.*

[273] *See* Satariano, *supra* note 264.

[274] *See Data Protection in Thailand: A Summary of the PDPA*, FOCAL POINT INSIGHTS (Oct. 24, 2019), https://blog.focal-point.com/data-protection-in-thailand-what-you-need-to-know-about-the-pdpa [https://perma.cc/H3LJ-N8TZ].

[275] *See* Claudia Rossi, *Data Protection 2019: Chile*, ICLG (Mar. 7, 2019), https://www.acc.com/sites/default/files/resources/upload/DP19_E-Edition.pdf [https://perma.cc/8APF-UJ3M].

[276] *See* Mario Rognoni, *Panama - The Impact of the GDPR Outside the EU*, LEXOLOGY (Oct. 8, 2019), https://www.lexology.com/library/detail.aspx?g=e138a075-95e2-4959-8498-696967e63d18 [https://perma.cc/FD36-39TX].

[277] *See* Alex Wall, *GDPR Matchup: South Korea's Personal Information Protection Act*, IAPP (Jan. 8, 2018), https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act [https://perma.cc/2TU3-YBQJ].

[278] *See* Yomi Kazeem, *Kenya is Stepping Up Its Citizens' Digital Security with a New EU-Inspired Data Protection Law*, QUARTZ AFR. (Nov. 12, 2019), https://qz.com/africa/1746202/kenya-has-passed-new-data-protection-laws-in-compliance-with-gdpr [https://perma.cc/HTQ9-S9V2].

[279] *See* Jehl & Friel, *supra* note 61.

[280] *See* Sarah Buerger, *How the GDPR Changed the Argentina Personal Data Protection Act*, MICHALSONS (Feb. 21, 2017), https://www.michalsons.com/blog/argentina-personal-data-protection-act/25090 [https://perma.cc/8FV9-VQ4W].

D. Serving as Examples

[53] Finally, more robust comprehensive data protection laws serve as models for subsequent laws in other jurisdictions.[281] For example, the GDPR has served as a prototype for comprehensive data protection legislation in countries from Asia to the Americas.[282] Indeed, the GDPR has been viewed as a particularly accessible model for adaptation.[283] It has had especially significant influence in Latin America, where Brazil's data privacy law mirrors the GDPR, and countries such as Chile, Argentina, and Mexico have increased their own privacy protections after the passage of the GDPR.[284]

[54] But beyond directly copying or being inspired by stricter data protection legislation like the GDPR , the proliferation of such laws can also serve as laboratories of democracy. Popularly coined by Justice Louis Brandeis in a 1932 U.S. Supreme Court case,[285] the idea of laboratories of democracy is for states to act as "laboratories" where policyexperiments can take place with little risk to the country at large.[286] This same laboratories of democracy concept can be applied in the international

[281] MULLIGAN ET AL., *supra* note 16, at 40.

[282] *Id.* at 50–51.

[283] Schwartz, *supra* note 21, at 810–811.

[284] Paulina Bojalil et al., *Data Privacy Reform Gains Momentum in Latin America*, ABIERTO AL PÚBLICO (Feb. 12, 2019), https://blogs.iadb.org/conocimiento-abierto/en/data-privacy-reform-gains-momentum-in-latin-america [https://perma.cc/Y2VP-LNZV].

[285] New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("[A] single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

[286] *See* Edmund Andrews, *Steven Callander: How to Make States "Laboratories of Democracy,"* INSIGHTS BY STAN. BUS. (May 19, 2015), https://www.gsb.stanford.edu/insights/steven-callander-how-make-states-laboratories-democracy [https://perma.cc/JER5-M26N].

data privacy context.[287] Countries such as the United States can observe the outcomes of data privacy regulation in jurisdictions with more stringent and comprehensive laws to see what works effectively and what falls short. This is especially true where discrepancies arise, such as a consumer's right to opt out of sales of their personal information, which is effectively included in the GDPR, PPDA, LGPD, PIPEDA, and Data Protection Act, but not the PPL, APPI, Privacy Act, or FADP.[288] This is also important for vague or ambiguous terminology in these acts; as time passes, courts will play a significant role in better defining these regulations,[289] and other jurisdictions can operate on this expanded knowledge. As more U.S. states follow California and adopt their own comprehensive data protection laws, these will serve as additional laboratories of democracy in a U.S. context.

V. Conclusion

[55] Although data protection law in the United States is fractured, and international law in the realm is nonexistent, foreign data protection laws are having a significant impact on the protection of U.S. consumers' personal data. A growing number of comprehensive data protection laws are emerging on every continent. The economic and social pressures to conform to more stringent data protection standards are resulting in a trend of GDPR-like data protection legislation becoming the global standard.[290] The influence of foreign data protection laws cannot replace the existence of a comprehensive data protection law in the United States, as gaps will

[287] *See* Joanne McNabb, *Can Laboratories of Democracy Innovate the Way to Privacy Protection?*, CENTURY FOUND. (Apr. 5, 2018), https://tcf.org/content/report/can-laboratories-democracy-innovate-way-privacy-protection/?agreed=1 [https://perma.cc/DE6J-HNVB].

[288] *E.g.*, Navdeep K. Singh, *What You Need to Know About the CCPA and the European Union's GDPR*, AMERICAN BAR ASSOCIATION (Feb. 26, 2020), https://www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2020/what-you-need-to-know-about-the-ccpa-and-the-european-unions-gdpr [https://perma.cc/G7NY-HZK4].

[289] *Will the EU's GDPR Rules Launch a New Era of Data Protection?*, *supra* note 233.

[290] *See* MULLIGAN ET AL., *supra* note 16, at 51.

remain in areas such as data localization requirements and enforcement. Nonetheless, these foreign laws, by forcing U.S. companies to comply with improved data protection standards, increasing consumer awareness, pressuring the U.S. government to improve data privacy regulations, and providing examples of successful legal models, are increasing the protection of U.S. consumers today and in the future.