Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 40 | Issue 1 Article 3

2024

ANALYSIS OF GLOBAL DATA PRIVACY REGULATIONS AND HOW TRANSNATIONAL COMPANIES ARE IMPACTED

Fujimori-Smith, Aska

ANALYSIS OF GLOBAL DATA PRIVACY REGULATIONS AND HOW TRANSNATIONAL COMPANIES ARE IMPACTED

Aska Fujimori-Smith[*]

Privacy regulations are being developed and altered globally. An American company working transnationally will want to make sure to comply with the privacy regulations of each country in which the company either conducts business or otherwise utilizes that country's citizens' data. Currently, the GDPR has the strictest standards regarding data processing agreements between a primary organization and another data processor. While the CCPA/CPRA and the PDPA require DPAs, a company in compliance with the GDPR will likely comply with the CCPA/CPRA and the PDPA. Case law is evolving to address the extent of the reach of the extraterritorial legislation. However, if a company is engaged in extensive data collection, then the company should ensure compliance with all relevant privacy regulations.

As new legislative responses emerge worldwide, it is crucial for companies engaged in international business transactions to ensure compliance with the different standards of that extraterritorial legislation.

[*] J.D. Candidate, Santa Clara University School of Law, 2024.

CONTENTS

I. INTRODUCTION

With the rise of global transactions between major companies, consumer data has become a dominant commodity for sale and transfer.[1] Privacy is a fundamental right recognized long before the collection and sale of data became pervasive.[2] In an instrumental law review article for privacy rights, Justice Louis Brandeis and Samuel Warren discuss the importance of the right "to be let alone," particularly as times change and evolving common law broadens the scope of legal rights to include privacy.[3] Additionally, the Universal Declaration of Human Rights adopted by the General Assembly of the United Nations in 1948 also includes the right to privacy.[4] Privacy has deep roots in historical, political, and religious backgrounds.[5] The issue of consumer data privacy is becoming increasingly scrutinized, and within the past few years, governments have begun intervening in the sale, usage, and disclosure of consumer personal information by passing major privacy protection laws.[6] For example, due to new privacy regulations, data processing agreements are now ubiquitous.[7] Yet, for many companies, the requirement of a data processing agreement was nonexistent just a few years ago.[8]

As governments worldwide implement new privacy regulations, the laws passed attempt to govern companies that do not

---

[1] *See* Jacques Bughin, Susan Lund & James Manyika, *Globalization is Becoming More About Data and Less About Stuff,* HARV. BUS. REV. (Mar. 14, 2016), https://hbr.org/2016/03/globalization-is-becoming-more-about-data-and-less-about-stuff.

[2] *See* Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); *Universal Declaration of Human Rights,* UNITED NATIONS, https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[3] Brandeis & Warren, *supra* note 2.

[4] *See Universal Declaration of Human Rights*, *supra* note 2.

[5] *See* DEBRAE KENNEDY-MAYO & PETER SWIRE, U.S. PRIVATE-SECTOR PRIVACY LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS 17 (3d ed. 2020).

[6] *See* Ruth Green, *Data Protection Shifts Up a Gear as Pressure Mounts on Governments to Regulate*, INT'L BAR ASS'N (Mar. 3, 2022), https://www.ibanet.org/data-protection-shifts-up-a-gear.

[7] *See* Michael Hahn, Sundeep Kapur & Matt Savare, *A Data Processing Addendum for the CCPA?*, IAPP PRIV. PERSPS. (June 19, 2019), https://iapp.org/news/a/a-data-processing-addendum-for-the-ccpa/.

[8] *See id.*

necessarily have a direct presence in the countries at issue.[9] Transnational companies must be attentive to the evolving landscape of privacy laws and ensure compliance with the requirements of various countries.

This note (1) traces the development and salience of the issue of consumer data privacy; (2) provides a global overview of currently enacted governmental privacy regulations; (3) provides an analysis of the regulations; and (4) discusses potential legislative responses, as well as how an international company can be compliant with various privacy protection laws.

II. HISTORICAL OVERVIEW OF CONSUMER DATA PRIVACY

The right to privacy is not a new concept. "Privacy is referenced numerous times in the laws of classical Greece and in the Bible . . . [and] in the Qur'an."[10] Additionally, the 1361 Justices of the Peace Act in England included the legal protection of privacy rights through the inclusion of "provisions calling for the arrest of 'peeping Toms' and eavesdroppers."[11] In 1976, the United Nations passed the International Covenant on Civil and Political Rights (ICCPR).[12] Article 17 of the ICCPR "protects everyone from arbitrary or unlawful interferences with their privacy, family, home or correspondence."[13]

Yet, since 1976, technology has developed rapidly, and with it, the deterioration of consumer privacy rights.[14] With innovations and technology, data collection and sale have become significantly easier, making consumer data a ubiquitous commodity.[15] Companies have tried to keep up with growing demands of data privacy protection

---

[9] *See* Alexander Garrelfs, *GDPR Top Ten #3: Extraterritorial Applicability of the GDPR*, DELOITTE, https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-extraterritorial-applicability.html (discussing how the GDPR is extraterritorial legislation); *see also* Maya Atrakchi et al., *Does the CCPA Apply to Your Business?*, NAT'L L. REV., https://www.natlawreview.com/article/does-ccpa-apply-to-your-business (considering the extraterritorial effect of the CCPA on businesses located outside of California).

[10] KENNEDY-MAYO & SWIRE, *supra* note 5.

[11] *Id.*

[12] *See The Human Right to Privacy in the Digital Age*, AM. CIV. LIBERTIES UNION (Mar. 25, 2015), https://www.aclu.org/documents/human-right-privacy-digital-age.

[13] *Id.*

[14] *See id.*

[15] *See* Nicholas G. Carr, *IT Doesn't Matter,* HARV. BUS. REV. (May 2003), https://hbr.org/2003/05/it-doesnt-matter.

through the implementation of information management programs and incorporation of privacy notices and privacy policies both externally and internally.[16] However, foreign and domestic governmental enforcement of privacy laws is prevalent and crucial to protect data privacy and promote company accountability.[17]

Even before the rise of the internet, data collection has been an integral part of the business process.[18] Companies constantly want to better anticipate the needs and desires of their consumers.[19] Data collection has allowed companies to achieve this by tracking customers' past orders and preferences.[20] Data collection has been crucial to the development of census-taking,[21] marketing and product development,[22] healthcare systems,[23] algorithmic anticipation of consumer needs,[24] and many other aspects of our daily lives.[25] With the rise of the internet and new technology, consumers now utilize

---

[16] *See* KENNEDY-MAYO & SWIRE, *supra* note 5, at 72–86.

[17] *See id.* at 28–32.

[18] *See* Swish Goswami, *The Rising Concern Around Consumer Data and Privacy*, FORBES (Dec. 14, 2020), https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/.

[19] *See id*.

[20] *See id*.

[21] *See* Julia Coombs & Misty L. Heggeness, *How We Develop and Improve the Census*, U.S. CENSUS BUREAU (July 31, 2019), https://www.census.gov/library/stories/2019/07/how-we-develop-improve-the-census.html.

[22] *See* Steven Rosenbush & Michael Totty, *How Big Data is Changing the Whole Equation for Business*, WALL ST. J. (March 10, 2013), https://www.wsj.com/articles/SB10001424127887324178904578340071261396666.

[23] *See* Roberta Pastorino et al., *Benefits and Challenges of Big Data in Healthcare: An Overview of the European Initiatives*, NAT'L LIBR. MED. (Oct. 29, 2019), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6859509/.

[24] *See* David Court et al., *Big Data, Analytics, and the Future of Marketing & Sales*, MCKINSEY & CO. (March 2015), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Marketing%20and%20Sales/Our%20Insights/EBook%20Big%20data%20analytics%20and%20the%20future%20of%20marketing%20sales/Big-Data-eBook.ashx.

[25] *See* Terence Mils, *Big Data is Changing the Way People Live Their Lives*, FORBES (May 16, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/05/16/big-data-is-changing-the-way-people-live-their-lives/?sh=f9e0a443ce67.

websites, applications, and cars daily—all of which collect personal identifiable information (PII).[26] Increasingly, consumer personal data, online behavior, and locations are being tracked and collected.[27] Governmental regulations are also increasing in the realm of data privacy so that "[w]here once companies were always ahead of regulators, now they struggle to keep up with compliance requirements across multiple jurisdictions."[28]

Data collection and exploitation have significant consequences to consumers. For instance, in the healthcare data sector, data can be utilized to improve the effectiveness and efficiency of healthcare systems.[29] Yet, healthcare data can also have detrimental ramifications, as well. Lack of privacy regarding healthcare data can restrict reproductive health services in certain regions.[30] Additionally, lack of patient trust towards medical doctors and the healthcare system may also prevent individuals from receiving necessary care.[31] Data privacy impacts our daily lives, and as data collection becomes easier and more efficient, it is crucial that governments further regulate data usage to prevent exploitation of consumer data.

As technology has become an integral part of our daily lives, consumers have become more aware of the possibility of data breaches and the extent of data collection, and they are taking steps to ensure their data privacy.[32] Consumer data is aggressively becoming "[a] new

---

[26] *See* Rob Shavell, *Privacy as a Growing and Changing Source of Business Risk*, FORBES (June 23, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/06/23/privacy-as-a-growing-and-changing-source-of-business-risk/.

[27] *See Consumer Data: Increasing Use Poses Risks to Privacy,* U.S. GOV'T ACCOUNTABILITY OFF. (Sep. 13, 2022), https://www.gao.gov/products/gao-22-106096.

[28] Alex Pentland & Hossein Rahnama, *The New Rules of Data Privacy*, HARV. BUS. REV. (Feb. 25, 2022), https://hbr.org/2022/02/the-new-rules-of-data-privacy.

[29] *See* Pastorino et al., *supra* note 23.

[30] *See Patient Survey Shows Unresolved Tension Over Health Data Privacy*, AM. MED. ASS'N (July 25, 2022), https://www.ama-assn.org/press-center/press-releases/patient-survey-shows-unresolved-tension-over-health-data-privacy.

[31] *See id.*

[32] *See* Venky Anant et al., *The Consumer-Data Opportunity and the Privacy Imperative*, MCKINSEY & CO. (April 27, 2020), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative.

commodity spawn[ing] a lucrative, fast-growing industry."[33] Simultaneously, governments have begun promulgating data privacy regulations to protect consumers from global conglomerates.[34] The ramifications of stringent data privacy laws can be extensive, impacting small, medium, and large companies across the world.[35] Data privacy has transformed from an industry-specific or deal-specific issue into an issue present in nearly every transaction.[36]

The most prominent data privacy protection law is the General Data Protection Regulation (GDPR) passed in the European Union (EU) in 2018.[37] In a phenomenon called "The Brussels Effect," the EU often promulgates sweeping influential regulations in many areas including privacy.[38] The purpose of the GDPR was to provide a comprehensive, overarching framework for privacy protection in the EU.[39] The seven principles identified in GDPR Article V are (1) lawfulness, fairness, and transparency; (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality (security); and (7) accountability.[40] Global companies who wish to partake in business within any member of the EU states

---

[33] *The World's Most Valuable Resource is No Longer Oil, But Data*, ECONOMIST (May 6 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[34] *See* Kristin M. Hadgis et al., *Data Privacy: Evolving Updates to the Global Landscape*, MORGAN LEWIS (Sept. 14, 2022), https://www.morganlewis.com/pubs/2022/09/data-privacy-evolving-updates-to-the-global-landscape.

[35] *See GDPR Small Business Survey,* GDPR.EU (May 2019), https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf.; *see also* Ivana Kottasova, *These Companies are Getting Killed by GDPR,* CNN BUS. (May 11, 2018), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html.

[36] *See* Matthew Bacal, Mikaela Dealissia & Pritesh Shah, *Private M&A: Data Privacy and Cybersecurity in Global Dealmaking*, LEXOLOGY (Oct. 3, 2022), https://www.lexology.com/library/detail.aspx?g=0e3896f6-55f8-40b5-a8e0-0682266a0ce9.

[37] *See* Ben Wolford, *What is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ (last visited July 17, 2023).

[38] Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2015).

[39] *See* Matt Burgess, *What is the GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (March 24, 2020), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

[40] *See id*.

must comply with the GDPR requirements, including putting in place written data processing agreements with data processors.[41]

In contrast, in the United States, rather than a general federal privacy law, there are instead individual laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Children's Online Privacy Protection Rule (COPPA), which cover data privacy in limited subject matters and in specific circumstances.[42] These piecemeal laws have not provided an overarching framework for consumer data protection outside of limited situations.[43] There have been discussions and proposals about potential federal regulations regarding consumer data privacy; however, none have yet gone into effect as law.[44] For example, in a Congressional hearing from 2019, committee members in Congress discussed the issue of protecting consumer privacy in the era of Big Data.[45] This discussion included the ease of collection and sale of data with modern technology.[46]

Some states enforce more comprehensive and dominant privacy laws, considering, in particular, California's two influential laws: the Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).[47] Taken together, both of these acts are the first comprehensive consumer privacy legislation in the United States.[48] The CCPA was enacted in 2018, and the CPRA was approved by a ballot

---

[41] *See* Ben Wolford, *What is a GDPR Data Processing Agreement?*, GDPR.EU, https://gdpr.eu/what-is-data-processing-agreement/ (last visited June 28, 2023); *see also* Ben Wolford, *Does the GDPR Apply to Companies Outside of the EU?*, GDPR.EU, https://gdpr.eu/companies-outside-of-europe/ (last visited June 28, 2023).

[42] *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why it Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

[43] *See id.*

[44] *See* Rebecca Kern, *Bipartisan Draft Bill Breaks Stalemate on Federal Data Privacy Negotiations*, POLITICO (June 3, 2022), https://www.politico.com/news/2022/06/03/bipartisan-draft-bill-breaks-stalemate-on-federal-privacy-bill-negotiations-00037092/.

[45] *See Protecting Consumer Privacy in the Era of Big Data*, *Hearing Before the Subcomm. on Consumer Prot. and Com. of the H. Comm. on Energy and Com.*, 116th Cong. 3 (2019).

[46] *See id*.

[47] *See* Klosowski, *supra* note 42.

[48] *See California Consumer Privacy Laws*, BLOOMBERG LAW, https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/ (last visited Jan. 28, 2023).

measure in 2020.[49] The CCPA and CPRA lay out specific rights for consumers and guidelines for companies in relation to selling or sharing consumer personal information.[50]

Another major privacy law is the Personal Data Protection Act of 2012 (PDPA) passed in Singapore. This act governs the collection, use, and disclosure of personal data by private companies,[51] but does not apply to public agencies.[52] Private companies that are governed by the PDPA must comply with the Act's requirements, such as implementing personal data protection policies within the company and designating a Data Protection Officer.[53]

With the development of new technology and business models, privacy laws are constantly being promulgated and amended.[54] The importance and salience of consumer data protection has pushed governments to pass regulations to attempt to control the flow of data.[55] Companies that engage in international transactions involving data flow must learn the ever-changing privacy requirements of various countries or risk being fined.[56]

III. OVERVIEW OF GDPR, CCPA & CPRA, AND THE PDPA

A significant concern that global companies face with the implementation of new privacy regulations is compliance with various countries' regulations.[57] Companies that conduct business and data collection, transfer, or sale within the specific jurisdictions will want to make sure to be compliant with the relevant privacy regulations.

---

[49] *See id.*

[50] *See id.*

[51] *See PDPA Overview,* PERS. DATA PROT. COMM'N SING., https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act (last visited June 28, 2023) [hereinafter *PDPA*].

[52] *See id*.

[53] *See Personal Data Protection Act (PDPA),* PWC, https://www.pwc.com/sg/en/personal-data-protection.html (last visited July 17, 2023).

[54] *See* Einat Weiss, *Data Privacy Rules Are Changing. How Can Marketers Keep Up?*, HARV. BUS. REV. (Aug. 27, 2020), https://hbr.org/2020/08/data-privacy-rules-are-changing-how-can-marketers-keep-up?ab=at_art_art_1x4_s03.

[55] *See* Green, *supra* note 6.

[56] *See PDPA*, *supra* note 51; *see also* Wolford, *What are the GDPR Fines?*, GDPR.EU, https://gdpr.eu/fines/ (last visited Aug. 24, 2023).

[57] *See* Hadgis et al., *supra* note 34.

First, the GDPR implemented in the EU is an example of extraterritorial legislation.[58] The GDPR greatly expanded Europe's previous privacy legislation, the Data Protection Directive, by expanding the scope of jurisdiction and making the GDPR applicable to companies that are based outside of the EU.[59] GDPR Article 3 Section 2 allows for this extraterritorial scope and states:

> This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> b) the monitoring of their behaviour as far as their behaviour takes place within the Union.[60]

Case law is still developing regarding the extent of the GDPR's extraterritorial reach. The case of *Soriano v. Forensic News* is helpful in determining the extent of the GDPR's reach.[61] In 2021, the High Court of England and Wales examined the extent to which Forensic News, a United States based news website defendant, could be subject to the GDPR's jurisdictional reach.[62] First, the Court concluded that Forensic News was not "established" within the EU for the purposes of GDPR jurisdiction, since the company did not "conduct minimal activity through stable arrangements" in the EU.[63] Next, the Court

---

[58] *See* Garrelfs, *supra* note 9.

[59] *See* Noriswadi Ismail & Catalina-Luisa Resmerita, *GDPR Extraterritoriality and Cross-Border Litigation*, AM. BAR ASS'N (July 3, 2019), https://www.americanbar.org/groups/litigation/committees/commercial-business/articles/2019/spring2019-gdpr-extraterritoriality-cross-border-litigation/.

[60] Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 3, 2016 O.J. (L 119) 1, 32-33 [hereinafter GDPR].

[61] *See* Claude-Etienne Armingaud & Noirin M. McFadden, *English High Court Examines Extent of GDPR's Extraterritorial Jurisdiction*, THE NAT'L L. REV. (March 5, 2021), https://www.natlawreview.com/article/english-high-court-examines-extent-gdpr-s-extraterritorial-jurisdiction.

[62] *See id*.

[63] *Id*.

determined that the company's activities were insubstantial in the United Kingdom, and that any offering of goods or services in the United Kingdom were "merely ancillary to [the company's] . . . core data processing activities at issue," and therefore, Article 3(2)(a) of the GDPR jurisdictional reach did not apply.[64] Finally, the Court concluded that Article 3(2)(b) of the GDPR jurisdictional reach did not apply because the company's use of cookies were not used "in relation to the type of profiling . . . the claimant took issue with" and instead "were used in the context of directing advertising content."[65]

This case helps set boundaries regarding the extraterritorial reach of the GDPR, particularly for non-European based companies who have minimal contacts with EU citizens.[66] However, an important consideration is whether other European courts will consider this case as binding or influential precedent, given the United Kingdom's departure from the European Union.[67] Until precedent within current European Union countries is set, it may be difficult to ascertain *Soriano*'s level of influence.[68]

In addition to its extraterritorial reach, the GDPR governs the processing of EU citizens and residents' data.[69] Specifically, Article 28, Section 3 governs data processing agreements:

> Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.[70]

A data processing agreement (DPA) is a "legally binding contract that states the rights and obligations of each party concerning the protection of personal data."[71] DPAs can be standalone agreements or added as an addendum to a business contract.[72] The GDPR requires

---

[64] *Id*.

[65] *Id*.

[66] *See id.*

[67] *See* Armingaud & McFadden, *supra* note 61.

[68] *See id.*

[69] *See* Wolford, *supra* note 37.

[70] GDPR, *supra* note 60, art. 28.

[71] Wolford, *supra* note 41.

[72] *See* Amal Ali et al., *Data Processing Agreements: The 10 Most Important Considerations*, COOLEY (Oct. 19, 2021),

written DPAs between companies and third-party businesses that process personal data, including data processors and subcontractors who process data.[73] To help determine who is a data processor, the GDPR broadly defines "processing" data as including the collection, storage, monetization, and destruction of data.[74]

Specifically, under Article 28 of the GDPR, there are eight topics that must be addressed in a DPA: (1) the processor agrees to process personal data only on written instructions of the controller; (2) confidentiality is required for all parties coming into contact with the data; (3) appropriate technical and organizational measures are utilized to protect the security of the data; (4) the processor will not subcontract to another processor, unless instructed to do so in writing by the controller, in which case another DPA will be required to be signed with the subcontractor; (5) the data processor will aid the controller in upholding the controller's obligations under the GDPR; (6) the processor will help the controller maintain GDPR compliance with regard to Article 32 and Article 36 of the GDPR (regarding the security of processing and consultation with data protection authority before undertaking high-risk processing); (7) the processor will agree to delete all personal data upon the termination of services or return the data to the controller; and (8) the processor must allow the controller to conduct an audit and will provide whatever information is necessary to prove compliance.[75]

Companies engaging in business transactions within the EU that collect, process, and otherwise disclose data must ensure that there are written DPAs in place with data processors that discuss the aforementioned requirements.[76] In addition, companies such as Box have made DPAs available to be signed easily by customers to show proof of GDPR compliance obligation.[77] Noncompliance with GDPR regulations will result in fines of "up to 4% of a company's annual

---

https://cdp.cooley.com/data-processing-agreements-the-10-most-important-considerations/.

[73] *See* Wolford, *supra* note 41.

[74] *See* Wolford, *supra* note 37.

[75] *See* Wolford, *supra* note 41.

[76] *See id.*

[77] *See* Katie Uhlman, *Box Leads Charge on GDPR With First-of-its-Kind Data Processing Addendum and New Global Data Protection Consulting Services,* BUS. WIRE (Feb. 15, 2018), https://www.businesswire.com/news/home/20180215005377/en/Box-Leads-Charge-on-GDPR-With-First-of-its-Kind-Data-Processing-Addendum-and-New-Global-Data-Protection-Consulting-Services.

global revenues or 20 million euros ($22.8 million), whichever is the bigger amount."[78]

In contrast, the CCPA and CPRA have different DPA requirements.[79] The CCPA and CPRA are applicable to private for-profit companies collecting or processing the data of California residents only.[80] Companies engaging in business transactions with California residents, which have a gross annual revenue of over $25 million; or buy, receive, or sell the personal information of 100,000 or more California residents, households, or devices; or derive 50% or more of their annual revenue from selling California residents' personal information, will want to assure compliance with the CCPA and CPRA.[81]

The CPRA created the California Privacy Protection Agency, an agency vested with authority, administrative power, and jurisdiction necessary to enforce the CCPA.[82] Taken together, the CCPA and CPRA create eight consumer rights, which are: (1) the right to know of personal information collected by the business about the consumer, from whom it was collected, why it was collected and if sold, to whom; (2) the right to delete personal information collected from the consumer; (3) the right to opt-out of the sale of personal information; (4) the right to opt-in to the sale of personal information of consumers under the age of sixteen; (5) the right to non-discriminatory treatment for exercising any rights; (6) the right to initiate a private cause of action for data breaches; (7) the right to correct inaccurate personal

---

[78] Ryan Browne, *Fines for breaches of EU privacy law spike sevenfold to $1.2 billion, as Big Tech bears the brunt,* CNBC (Jan. 17, 2022), https://www.cnbc.com/2022/01/18/fines-for-breaches-of-eu-gdpr-privacy-law-spike-sevenfold.html.

[79] See David Stauss & Mike Summers, *How do the CPRA, CPA & VCDPA Treat Data Processing Agreements?*, HUSCH BLACKWELL (Mar. 22, 2022), https://www.bytebacklaw.com/2022/03/how-do-the-cpra-cpa-and-vcdpa-treat-data-processing-agreements/; *see also* David Stauss & Malia Rogers, *Analyzing the CPRA's New Contractual Requirements for Transfers of Personal Information*, IAPP (Mar. 23, 2021), https://iapp.org/news/a/analyzing-the-cpras-new-contractual-requirements-for-transfers-of-personal-information/.

[80] *See Who is Covered by CPRA (formerly CCPA) and What Does It Require?*, DOCUSIGN (Aug. 8, 2022), https://www.docusign.com/blog/who-is-covered-by-ccpa-and-what-does-it-require.

[81] *See California Consumer Privacy Laws*, *supra* note 48.

[82] *See id.*

information; and (8) the right to limit use and disclosure of sensitive personal information.[83]

Data processing agreements under the CCPA and CPRA must prohibit the service provider (data processor) from (1) selling or sharing the personal information; (2) retaining, using, or disclosing personal information outside of the direct business relationship between the service provider and the business; (3) retaining, using, or disclosing the personal information for any other purpose than that specified in the contract between the business and contractor or service provider; and (4) combining personal information received from one business with information received from another business.[84] In addition, companies who receive deletion requests of personal data by a California resident must also "notify . . . their own service providers or contractors to delete the [consumer's] personal information."[85] A distinction from the GDPR is that it is unclear to what extent the California laws regulate downstream data processors.[86] For example, service providers are not required to "flow down their prohibitions to other service providers."[87]

The CCPA and CPRA DPA requirements are different from the GDPR DPA requirements.[88] Businesses engaging in transactions involving California residents' personal information must ensure they comply with California requirements for a contract between the company and service provider, or other third party.[89]

Next, Singapore's Personal Data Protection Act (PDPA) is another globally influential privacy regulation. The PDPA applies to all organizations that collect, use, or disclose personal data in Singapore, regardless of the organization's home country.[90] Regarding data exports, the PDPA requires that "the standard of protection at the receiving . . . [country] is comparable to protections under the PDPA."[91]

---

[83] *See id.*

[84] *See* Stauss & Summers, *supra* note 79.

[85] *Id.*

[86] *See* Hahn, Kapur & Savare, *supra* note 7.

[87] *Id.*

[88] *Compare* Wolford, supra note 41, *with* Stauss & Summers, *supra* note 79; Stauss & Rogers, *supra* note 79.

[89] *See California Consumer Privacy Laws*, supra note 48.

[90] *See Data Protection Laws of the World*, DLA PIPER (Dec. 21, 2021), https://www.dlapiperdataprotection.com/index.html?t=law&c=SG&c2=.

[91] Yoolim Lee, *Singapore Cos Listing Abroad Are Subject to Data Protection Laws*, BLOOMBERG LAW (July 27, 2021),

Companies can achieve this standard by strategically implementing clauses into contracts or binding corporate rules.[92] Under the PDPA, written contracts between the primary organization and "data intermediaries" are required.[93] Data intermediaries refers to "an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation."[94] While the compliance requirements for data intermediaries are less stringent compared to those that a primary organization must meet, data intermediaries must still comply with rules regarding the protection and retention of personal data, and they have a duty to notify the primary organization of a data breach.[95] Thus, the PDPA imposes certain obligations on data intermediaries, yet the Act does not appear to have as stringent DPA requirements as the GDPR requires.[96]

The GDPR, CCPA/CPRA, and the PDPA all have data protection requirements, particularly when companies utilize other data processing parties to handle the consumer data.[97] The GDPR appears to have the strictest requirements for DPAs between a company and another data processor by making many aspects of the written agreement compulsory.[98] The purpose of these DPAs is to further the broader objectives of the privacy regulations, which is to allow consumers to assert certain rights and ensure that consumer data is transferred, processed, or handled in a proper and secure manner.[99]

---

https://news.bloomberglaw.com/privacy-and-data-security/singapore-cos-listing-abroad-are-subject-to-data-protection-laws.

[92] *See id.*

[93] Chong Kin Lim, DATA PROTECTION & PRIVACY 2019, GETTING THE DEAL THROUGH 169, 174.

[94] Chong Kin Lim, *Singapore - Data Protection Overview*, ONETRUST DATAGUIDANCE (May 2022), https://www.dataguidance.com/notes/singapore-data-protection-overview.

[95] *See* Lim, *supra* note 93, at 174.

[96] *See id.*

[97] *See* Lim, *supra* note 94; *California Consumer Privacy Laws*, *supra* note 48; Wolford, *supra* note 41.

[98] *Compare* Wolford, *supra* note 41, *with* Lim, *supra* note 94, *and California Consumer Privacy Laws*, supra note 48.

[99] *See* Wolford, *supra* note 41.

IV. ANALYSIS REGARDING ENSURING COMPLIANCE WITH ALL REGULATIONS

Global companies often face tension in determining what jurisdictions' regulations and laws they should comply with. Specifically, Article 3 of the GDPR makes the GDPR applicable to non-EU-based organizations that are not physically established in the EU.[100] Thus, companies outside of the EU can still fall under the regulations of the GDPR and must comply with the law.[101]

The case of *Hartford Fire Insurance v. California* is instructive in determining when the principle of international comity may not apply and when a United States court can still exercise subject matter jurisdiction over a case.[102] At issue in *Hartford Fire Insurance* was an alleged violation of the Sherman Act by Defendants, by engaging in various conspiracies to impact the American insurance market.[103] There, the foreign defendants, London reinsurance companies, argued that their behavior was acceptable under a comprehensive British regulatory scheme, and thus the principle of international comity should apply and the United States court should not exercise jurisdiction over the case.[104]

The Supreme Court held that the principle of international comity should not deter a court in the United States from exercising subject matter jurisdiction over a case if it is possible to comply with both domestic and international law.[105] "The fact that conduct is lawful in the state in which it took place will not, of itself, bar application of the United States antitrust laws, even where the foreign state has a strong policy to permit or encourage such conduct."[106] Although the alleged conspiracies were permissible under British law, the foreign defendants did not argue that "British law requires them to act in some fashion prohibited by the law of the United States."[107] Furthermore, where "[n]o conflict exists . . . a person subject to regulation by two states can comply with the laws of both."[108]

---

[100] *See* Ismail & Resmerita, *supra* note 59.

[101] *See id.*

[102] *See Hartford Fire Ins. Co. v. California*, 509 U.S. 764, 769–70 (1993).

[103] *See id*. at 770.

[104] *See id.* at 797–99.

[105] *See id.* at 799.

[106] *Id.*

[107] *Hartford Fire Ins. Co. v. California*, 509 U.S. 764, 769–70 (1993).

[108] *Id.*

Similarly, there appears to be no conflict between the GDPR, CPRA/CCPA, and PDPA regarding data processing agreements.[109] Although the GDPR has the most stringent requirements, setting out many necessary provisions of a DPA, a DPA in compliance with the GDPR will likely be in compliance with the CPRA/CCPA and PDPA.[110] Therefore, global companies conducting international business transactions concerning consumer data of EU citizens, California citizens, or within Singapore can comply with the DPA requirements set forth in the respective countries' privacy regulations without having conflicting requirements.[111]

Furthermore, the GDPR, CPRA/CCPA, and PDPA are made applicable to certain transactions due to the subject matter and data collection of citizens thereof.[112] Therefore, companies cannot simply choose a choice of law clause of another country with less stringent privacy requirements in order to prevent being subject to the privacy laws in the EU, California, and Singapore. Companies are expected to comply with the applicable privacy regulations.

For example, recently, X (formally known as Twitter), a globally popular social media company, has come under scrutiny by both the United States and European Union officials to ensure compliance with privacy regulations.[113] Namely, the resignations of X's Chief Privacy Officer and Chief Compliance Officer have led to the United States Federal Trade Commission (the agency in charge of regulating and overseeing how X handles user data and data security compliance) making a statement discussing "deep concern" regarding X's management.[114] X is also under scrutiny in Europe and is scheduled

---

[109] *See* Lim, *supra* note 94; *California Consumer Privacy Laws*, *supra* note 48; Wolford, *supra* note 41.

[110] *See supra* note 109.

[111] *See id.*

[112] *See* Ismail & Resmerita, *supra* note 59; Atrakchi et al., *supra* note 9; *PDPA Overview, supra* note 51.

[113] *See* Stephanie Bodoni, *Twitter Called to Meet EU Data Watchdog Over Privacy Concerns*, BLOOMBERG LAW (Nov. 11, 2022), https://www.bloomberg.com/news/articles/2022-11-11/twitter-called-to-meet-eu-data-watchdog-over-privacy-concerns; *see also* Thomas Seal, *Twitter's Hectic Overhaul Puts World's Regulators on Alert (1)*, BLOOMBERG LAW (Nov. 11, 2022), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/ (search for title of article in search bar; select article from search results).

[114] Seal, *supra* note 113.

to meet with its European Union data protection watchdog in the future concerning the safety of users' personal data.[115]

Furthermore, various American companies have been fined for noncompliance with the GDPR.[116] According to a report in 2019 by the United States International Trade Commission, since May 2018, the second and third largest fines imposed on GDPR violations were imposed on "U.S.-based multinational companies Google and Marriot."[117] Enforcement of extraterritorial legislation has been trending upwards towards more imposition of fines against companies in violation of privacy laws.[118] In addition to the fines already imposed on U.S.-based companies, there are a number of ongoing GDPR investigations against U.S. firms, specifically many U.S.-based technology companies, such as Facebook, WhatsApp, Instagram, X, LinkedIn, Apple, Google, and Verizon.[119]

V. POTENTIAL LEGISLATIVE RESPONSES

Privacy law is constantly evolving and requires flexible, adaptive standards. Privacy is a unique area of regulation particularly because it transcends traditional boundaries; unlike other regulations, which may remain within a country's domestic boundary, the influential privacy regulations thus far have been extraterritorial in nature.[120] To be impactful, a country's legislation will need to regulate global companies that do not necessarily have a physical presence within the country's borders.[121]

Within the United States, the likely progression of legislative responses will culminate with a federal privacy regulation which will preempt most state privacy laws.[122] Currently, the American Data

---

[115] *See* Bodoni, *supra* note 113.

[116] *See* Brian Daigle & Mahnaz Khan, *One Year In: GDPR Fines and Investigations Against U.S.-Based Firms*, U.S. LAW INT'L TRADE COMM'N , Sept. 2019, https://www.usitc.gov/publications/332/executive_briefings/gdpr_enforcement.pdf.

[117] *Id.*

[118] *See id.*

[119] *See id.*

[120] *See* Garrelfs, *supra* note 9; Atrakchi et al., *supra* note 9; *PDPA Overview, supra* note 51.

[121] *See supra* note 120.

[122] *See Overview of the American Data Privacy and Protection Act, H.R. 8152*, CONG. RSCH. SERV. LEGAL SIDEBAR (Aug. 31, 2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10776.

Privacy and Protection Act (ADPPA) is "a proposed landmark U.S. federal privacy legislation that follows in the footsteps of the European Union's General Data Protection Regulation (GDPR)."[123] The ADPPA was approved by the House Committee on Energy and Commerce and will be sent to the U.S. House of Representatives for a vote.[124]

Although there is tension between state privacy rights and enforcement with a potential federal regulation, the independent states' privacy laws will likely not be sustainable in the long run because compliance with potentially fifty different state standards within the United States will be an arduous task in and of itself. Therefore, if a federal privacy regulation is passed, it will likely preempt state privacy laws.[125] For this reason, some states, such as California, who have already passed their own extensive privacy regulations, are hesitant in supporting a federal privacy law.[126] However, the new federal privacy law can include a "savings clause" which indicates that the federal privacy law is not intended to preempt any state privacy laws.[127] This will ensure that the federal privacy regulation establishes a minimum companies must follow, in addition to any other standards state laws already in place or that will be passed in the future will supplement. In this case, companies will need to ensure compliance with both federal level and state level privacy laws.

The intricacy and complexity of privacy law makes it difficult for companies to comply with all laws, some of which are being amended within a short time frame. Thus, if the United States is to implement a federal level privacy regulatory scheme, then it would be most effective to follow guidelines similar to the GDPR.

Often, when the EU implements a spearheading approach to regulations regarding general welfare, many countries follow in their

---

[123] Aysha F. Allos, *American Data Privacy and Protection Act: Are We Finally Getting Federal Data Privacy Protection?*, THE NAT'L L. REV. (Sept. 21, 2022), https://www.natlawreview.com/article/american-data-privacy-and-protection-act-are-we-finally-getting-federal-data-privacy.

[124] *See id.*

[125] *See id.*

[126] *See* Maria Curi, *California Clout on Data Privacy Poised to Weaken in GOP House*, BLOOMBERG LAW (Nov. 18, 2022), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/ (search for title of article in search bar; select article from search results).

[127] Dan Schweitzer, *The Law of Preemption*, NAT'L ATT'Y GEN. TRAINING & RSCH INST. (Oct. 2011), https://www.naag.org/wp-content/uploads/2020/10/The-Law-of-Preemption-2d-ed.-FINAL.pdf

footsteps.[128] The United States implementing policy similar to the EU will benefit not only American companies, but also companies conducting business transnationally. Compliance with both sets of laws would more likely be met since compliance with one would automatically mean compliance with another. Specifically, American companies who have already shifted approaches to comply with European laws in Europe can easily implement privacy regulation procedures and agreements in compliance with federal regulation within the United States.

Adoption of a similar set of privacy regulations to the GDPR will also prevent the principle of international comity from preventing the adjudication of a case within United States courts. Varying degrees of regulation or requirements may lead to conflicts of laws between countries, which will be difficult for large companies to accommodate. Thus, consistency in privacy approaches will augment compliance and legitimacy to both statutory schemes.

Furthermore, if the United States and the European Union adopt an identical set of privacy laws, this may encourage other countries to adopt similar privacy laws. While currently, there are variations of privacy law, since privacy is an issue that has global ramifications, consistency for standards of regulation will be helpful in ensuring compliance. If the United States and European Union—powerhouses in the global economy—follow similar regulations, other countries with developing privacy laws may be motivated to adopt similar regulations.

Another potential avenue to increase data flow and trade relations between the United States and the European Union would be to promulgate a new version of the U.S.-E.U. Privacy Shield.[129] Previously, the United States and European Union engaged in talks of a U.S.-E.U. Privacy Shield.[130] The Privacy Shield was intended to provide companies in the United States and the European Union with a "mechanism to comply with data protection requirements when transferring personal data" from the European Union and Switzerland to the United States.[131] Although in 2016 the European Commission approved data transfers under E.U. law between the two regions pursuant to the Privacy Shield, in 2020, the Court of Justice of the

---

[128] *See* Bradford, *supra* note 38.

[129] *See* Kristin Archick & Danielle M. Trachtenberg, *U.S.-EU Trans-Atlantic Data Privacy Framework*, CONG. RSCH. SERV. (June 2, 2022), https://crsreports.congress.gov/product/pdf/IF/IF11613.

[130] *See Privacy Shield Program Overview*, PRIV. SHIELD FRAMEWORK, https://www.privacyshield.gov/program-overview (last visited July 30, 2023).

[131] *Id.*

European Union invalidated the U.S.-EU. Privacy Shield Framework.[132] The Court concluded that the Privacy Shield Framework did not adequately comply with E.U. data protection requirements in data transfers with the United States.[133]

Similarly, the United States had engaged in a Swiss-U.S. Privacy Shield, yet the Swiss-U.S. Privacy Shield Framework was later invalidated by the Federal Data Protection and Information Commissioner of Switzerland in 2020, holding that the Privacy Shield Framework did not provide an "adequate level of protection for data transfers from Switzerland to the United States."[134]

The invalidation of these Privacy Shields is indicative of Europe's strong stance on data protection and desire to maintain control over transatlantic data flow. With the abrogation of the Privacy Shields, companies will want to ensure continued compliance with the relevant privacy regulations, namely the GDPR.

Currently, the United States and the European Union are working on a new Trans-Atlantic Data Privacy (TADP) Framework.[135] Certain companies, such as Meta, have threatened to withdraw from the EU market if a new TADP Framework agreement could not be reached.[136] A revamped Privacy Shield that adequately provides data protection for data import and export between the two regions will positively impact economic relations and facilitate secure data transfers.[137] The new TADP Framework would include more mandatory principles, including "provisions on sensitive data, secondary liability, the role of data protection authorities, human resources data," and many more.[138] The new Framework is also set to limit and safeguard data flow to any U.S. government surveillance agencies.[139] Furthermore, compliance with data flow standards under the new TADP Framework may encourage the United States to pass federal privacy regulations in line with the principles addressed in the agreement. If a TADP Framework agreement can be reached, then potentially global companies may engage in data privacy collection and

---

132 *See id.*

133 *See id.*

134 *Id.*

135 *See* Archick & Trachtenberg, *supra* note 129.

136 *See id.*

137 *See id.*

138 *Id.*

139 *See id.*

distribution between the United States and the EU according to Framework guidelines.[140]

Another potential policy change, on a global level, would be for the United Nations Human Rights Committee to update the General Comment with regards to Article 17 of the ICCPR to clearly define the "right to privacy" in a modern context with the understanding of the perils of privacy issues today, given rapid technological innovations.[141] The right to privacy is grounded in history throughout the world, yet the United Nations has not formally adopted the definition of the "right to privacy" in a 21st-century context.[142] Although General Comments are not necessarily binding, they are influential in helping interpret provisions of various "human rights treaty provisions and thematic issues."[143] General Comments can also guide states by "suggesting approaches to the implementation of the treaty provisions."[144] Thus, General Comments can be important in helping shape global approaches to privacy.

With the emergence of informational privacy as a "distinct and fundamental right," the General Comment must be updated to consider the current landscape of mass consumer data collection, retention, and usage.[145] The General Comment as-is fails to address the nexus between privacy rights and other fundamental rights, including the freedom of expression.[146]

Furthermore, as technology changes the way states, individuals, and companies interact with one another, surveillance by private or public entities can lead to severe consequences.[147] State surveillance, for example, has been made significantly easier with new technologies, which may further the power of authoritative states.[148] A

---

[140] *See id.*

[141] *The Human Right to Privacy in the Digital Age, supra* note 12.

[142] *See id.*

[143] Marite Decker & Stig Langvad, *The Purpose and Use of UN Treaty Body General Comments*, EUR. NETWORK ON INDEP. LIVING (Nov. 8, 2018), https://enil.eu/the-purpose-and-use-of-un-treaty-body-general-comments/.

[144] *Id.*

[145] *The Human Right to Privacy in the Digital Age, supra* note 12.

[146] *See id.*

[147] *See* Zeynep Tufekci, *We Need to Take Back Our Privacy,* N.Y. TIMES (May 19, 2022), https://www.nytimes.com/2022/05/19/opinion/privacy-technology-data.html.

[148] *See* Erica Frantz, Andrea Kendall-Taylor, & Joseph Wright, *The Digital Dictators: How Technology Strengthens Autocracy*, FOREIGN AFFS.

General Comment coming from a well-regarded international organization will be helpful in defining informational privacy as a foundational right, in establishing ground rules for public and private entity surveillance, and granting privacy a global credibility as a salient and crucial issue. Furthermore, the United Nations Human Rights Committee can also discuss the issue of international comity in an updated General Comment regarding privacy regulations. Privacy regulations promulgated by various countries necessarily are extraterritorial legislation. Discussing boundaries regarding future legislation will be helpful in navigating foreign laws and judicial systems.

Another consideration is that differences in culture and history between countries can impact their treatment of privacy rights and personal data.[149] For example, nations with a repressive history due to state surveillance and utilization of medical records or other data, may be more in favor of stringent privacy laws.[150] In Hungary, for instance, medical records are strongly protected under privacy rights because "dental records were used by the Kremlin in the Soviet era to identify…and kill [dissidents]."[151] In Germany, modern data protection laws that were enacted were motivated in part "[t]o prevent a reoccurrence of the personal information abuses that took place under Hitler's Third Reich before and during World War II."[152]

Given the weight and impact of history on privacy regulations, particularly in states with previously oppressive regimes, it will be substantially more difficult to promulgate privacy regulations on an international level. However, the United Nations is an appropriate, renowned body with a strong reputation to help bridge the gaps between countries with regards to privacy. The United Nations Human Rights Committee can help navigate countries with nascent privacy laws towards a regulatory scheme in line with principles of human rights protection by producing an updated General Comment regarding the right to privacy and discussing ways states may protect the privacy rights of their citizens.

(Feb. 6, 2020), https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators.

[149] *See* Monica Bay, *Law Tech: Privacy Laws are E-Discovery's Biggest Quandary*, BLOOMBERG LAW (Dec. 17, 2012), https://www.bloomberglaw.com/product/blaw/document/XA7P9S90000000.

[150] *See id.*

[151] *Id.*

[152] KENNEDY-MAYO & SWIRE, *supra* note 5.

VI. CONCLUSION

Privacy regulations are being developed and altered globally.[153] An American company working transnationally will want to make sure to comply with the privacy regulations of each country in which the company either conducts business or otherwise utilizes that country's citizens' data.[154] Currently, the GDPR has the strictest standards regarding data processing agreements between a primary organization and another data processor. While the CCPA/CPRA and the PDPA require DPAs, a company in compliance with the GDPR will likely comply with the CCPA/CPRA and the PDPA. Case law is evolving to address the extent of the reach of the extraterritorial legislation. However, if a company is engaged in extensive data collection, then the company should ensure compliance with all relevant privacy regulations.

As new legislative responses emerge worldwide, it is crucial for companies engaged in international business transactions to ensure compliance with the different standards of that extraterritorial legislation.

---

[153] *See* Hadgis et al., *supra* note 34.

[154] *See GDPR Compliance Checklist for US Companies*, GDPR.EU, https://gdpr.eu/compliance-checklist-us-companies/.