Washington Journal of Law, Technology & Arts

Volume 15 | Issue 2 Article 3

4-3-2020

Emerging Privacy Legislation in the International Landscape: Strategy and Analysis for Compliance

Jonathan McGruer

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 15, ISSUE 2 WINTER 2020

EMERGING PRIVACY LEGISLATION IN THE INTERNATIONAL LANDSCAPE: STRATEGY AND ANALYSIS FOR COMPLIANCE

Jonathan McGruer[*]

CITE AS: J MCGRUER, 15 WASH. J.L. TECH. & ARTS 120 (2020)
https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1303&context=wjlta

ABSTRACT

Big data is a part of our daily reality; consumers are constantly making decisions that reflect their personal preferences, resulting in valuable personal data. Facial recognition and other emerging technologies have raised privacy concerns due to the increased efficiency and scope which businesses and governments can use consumer data. With the European Union's General Data Protection Regulation ushering in a new age of data privacy regulation, international jurisdictions have begun implementing comparable comprehensive legislation, affecting businesses globally. This Article examines the similarities between emerging U.S. state data privacy laws and the General Data Protection Regulation, with suggestions for businesses implicated by emerging legislation. In addition is a comparative analysis of proposed and implemented foreign data privacy laws that may impact private companies considering investment or expansion into foreign markets.

[*] Jonathan McGruer, Managing Editor of the *Washington Journal of Law, Technology & Arts*. Thank you to the members of WJLTA for your help in bringing this article to publication.

TABLE OF CONTENTS

INTRODUCTION

The General Data Protection Regulation (the "GDPR") replaced the 1995 Data Protection Directive on May 25, 2018, resulting in a surge of private-sector investments in data privacy compliance programs, as well as bolstered consumer awareness regarding their rights to data protection.[1] The GDPR aims to harmonize data protection principles across EU Member States with a standardized regulatory framework. Furthermore, the expansive cross-border enforcement capabilities of the GDPR reaches private sectors foreign to the EU, inspiring governmental and private bodies to participate in cooperative regulation, and to ultimately draft new data privacy laws.

Privacy professionals and private businesses continue to display compliance concerns following the implementation of the GDPR.[2]

---

[1] *See* Jenifer Bauer, *How the GDPR Raises Public Awareness About Privacy*, NOWSECURE (Mar. 20, 2019), https://www.nowsecure.com/blog/2019/03/20/how-the-gdpr-raises-public-awareness-about-privacy/.

[2] *See* Samantha Ann Schwartz, *5 GDPR Pains That Won't Go Away*, CIO DIVE (Oct. 8, 2019), https://www.ciodive.com/news/5-gdpr-pains-that-wont-go-away/564470/.

Specifically, there are concerns regarding costs to companies from the implementation of GDPR-compliant data protection programs.[3] Despite these costs, many agree that there is significant economic potential tied to the increased analysis of big data,[4] in part due to standardized international data transfer guidelines, including Standard Contractual Clauses ("SCCs").[5] Businesses have included clauses approved by regulators in such agreements between service providers and customers to acceptably comply with agreements to transfer consumer data abroad.[6] In addition to implementation costs, jurisdictions' new comprehensive privacy laws do not consistently enforce the principles of the GDPR.[7] The EU Commission has

---

[3] *See* Samantha Ann Schwartz, *Why 67% of Companies Fear They Can't Sustain Privacy Compliance: True Privacy Depends on Where and How Data Travels*, CIO DIVE (Feb. 12, 2020), https://www.ciodive.com/news/data-privacy-CCPA-GDPR-fines/572077/.

[4] *See* Jesper Zerlang, *GDPR: A Milestone in Convergence for Cyber-Security and Compliance*, LOGPOINT (June 2017), http://isiarticles.com/bundles/Article/pre/pdf/128436.pdf ("While GDPR adherence may be a costly process for organisations focusing solely on 'ticking the box', the process can go beyond compliance. Instead, businesses can take advantage of the digitalisation process that GDPR encourages, utilising advanced tools to analyse [big data].").

[5] *Schrems II and Standard Contractual Clauses –the Advocate-General's Opinion*, ROPES & GRAY (Jan. 8, 2020), https://www.ropesgray.com/en/newsroom/alerts/2020/01/Schrems-II-and-Standard-Contractual-Clauses-the-Advocate-Generals-Opinion ("Many organisations rely on [Standard Contractual Clauses] as being a… cost-effective method of ensuring compliance with their data protection obligations regarding internationally transferred personal data.").

[6] *See European Union Model Clauses*, MICROSOFT (Jan. 28, 2020), https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-eu-model-clauses.

[7] *See* Detlev Gabel & Tim Hickman, *Chapter 15: Cooperation and Consistency – Unlocking the EU General Data Protection Regulation*, (Apr. 5, 2019), WHITE & CASE (Apr. 5, 2019), https://www.whitecase.com/publications/article/chapter-15-cooperation-and-consistency-unlocking-eu-general-data-protection ("Even if the applicable national data protection laws set similar standards across all Member States, enforcement requirements, attitudes, and standards may vary from Member State to Member State."), *available at* https://www.whitecase.com/publications/article/chapter-15-cooperation-and-consistency-unlocking-eu-general-data-protection.

worked to bridge potential gaps by giving authority to the European Data Protection Board to resolve issues of conflicting interpretations of data protection laws, hopefully guiding companies to respond properly to developing privacy regulations.[8] The GDPR represents the early international acceptance of a standard set of data protection principles, creating a clear foundation of consumer rights upon which legislatures and regulatory bodies can collaboratively base new privacy laws and enforcement mechanisms.

Enforcement of the GDPR has necessitated companies' formation of good data protection practices, as many penalties have been levied to date.[9] The GDPR has cost the average Fortune 500 company $16 million,[10] as significant investments by the private sector in technology and services have been required to create functionality for the efficient transfer and protection of consumer data. Further, the GDPR has a clear influence on foreign legislators' drafting of privacy laws. New privacy laws have emerged in the U.S. and internationally, many of which stress key principles of the GDPR, and address consumers' concerns regarding the public and private use of their personal information.[11]

This article begins in Part I by addressing the shift of consumers' focus post-GDPR towards the importance of having control over and knowing the extent to which their data is processed. Part I further examines enforcement and regulatory mechanisms of the GDPR, as well as key aspects of recommended risk assessment and privacy compliance programs. Following this overview of the GDPR, Part II introduces the push of EU privacy norms to the U.S., resulting in consumers' changed perception of data privacy expectations. New and proposed privacy laws in the U.S. are addressed. Part III considers the future of the GDPR enforcement,

---

[8] *Id.*

[9] *See GDPR Enforcement Tracker*, https://www.enforcementtracker.com (last visited Feb. 1, 2020).

[10] *See* Oliver Smith, *The GDPR Racket: Who's Making Money From This $9bn Business Shakedown*, FORBES (May 2, 2018), https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown.

[11] *See infra* Part III.

EU Commission "adequacy decisions," and potential problems surrounding aspects of emerging foreign data privacy laws.

I. THE GENERAL DATA PROTECTION REGULATION

An increase in consumer awareness following high-profile data breaches brought privacy concerns to the forefront of technology-related discussions, changing how consumers, businesses, and governments interoperate and handle information. [12] One consequence of developing technologies is the phenomenon of "Big Data," or the nearly "ubiquitous collection of data" about consumers, in conjunction with low storage costs and new data mining and profiling techniques available to businesses, resulting in heightened capabilities to analyze consumer data.[13] As consumers continue to utilize increasingly sophisticated technologies in their private lives, such as wearable devices and health and medical-related applications, the acquisition of personal data is increasingly necessary to meet consumer expectations, resulting in data security concerns.[14] Wearable technology and healthcare services delivered through mobile applications provide care at reduced costs. [15] In addition, medical applications allow doctors to provide care to rural or otherwise disadvantaged communities without requiring patients to travel to major city hubs.[16] Alongside the increase of consumers

---

[12] *See* Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, THE NEW YORK TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[13] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, at 1, (May 2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[14] *See* Alexy Sysoev, *Health and Fitness E-Gear Come With Security Risks*, THE INNOVATION ENTER. (Feb. 12, 2020), https://channels.theinnovationenterprise.com/articles/health-and-fitness-e-gear-brings-security-risks-in-post-new-year-days.

[15] *Opinion of the European Data Protection Supervisor on Mobile Health*, at 3, (May 21, 2015), https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf.

[16] *See* CENTERS FOR DISEASE CONTROL AND PREVENTION, TELEHEALTH IN RURAL COMMUNITIES, (May 31, 2019),

using technology that collects personal information is a newfound concern for data privacy, specifically protection from unwanted profiling, which exposes consumers to targeted advertising and other unwanted marketing strategies. Today, consumers are playing a balancing game. The availability of wearable technologies is exploding, introducing conveniences that are becoming a part of consumers' everyday lives. At the same time, use requires consumers to input a degree of highly personal and identifying information. Requiring consumers to choose between giving up their privacy and enjoying new technologies may be unreasonable, and new privacy laws relieve this tension.

The GDPR has two goals: (1) to protect consumers' fundamental rights to data protection, and (2) to ensure the free flow of personal data between Member States.[17] Parties operating physically outside of EU member states are not exempt from the GDPR due to its exterritorial applicability.[18] The GDPR provides for many of the same requirements as Directive 95/46, including consent-based processing, and data protection impact assessments.[19] Despite these subject matter similarities to Directive 95/46, the GDPR expanded obligations on businesses for each of those themes,[20] and provides

---

https://www.cdc.gov/chronicdisease/resources/publications/factsheets/telehealth-in-rural-communities.htm.

[17] Commission Regulation 2016/679, 2016 O.J. (L 119) 1, 1 [hereinafter GDPR].

[18] *See e.g.*, Alexander Garrelfs, *GDPR Top Ten #3: Extraterritorial Applicability of the GDPR*, DELOITTE (Apr. 3, 2017), https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-extraterritorial-applicability.html. Before the GDPR, privacy laws weren't applicable in many cases to controllers and processors outside of the EU. The GDPR provides for enforcement against companies that misuse consumer personal information by (1) targeting EU citizens; or (2) monitoring EU citizens. The author recommends organizations established outside of the EU to determine whether GDPR obligations apply to them.

[19] Directive 95/46/EC, 1995 O.J. (L 281) 2(h), 17, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.

[20] *See* Ivan Klekovic, *EU GDPR vs. European Data Protection Directive*, EU GDPR ACADEMY: EU GDPR BLOG (Oct. 30, 2017), https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/.

for much more significant enforcement measures to be levied should these obligations be breached.[21]

The GDPR codifies principles of fundamental rights pursuant to the Charter of Fundamental Rights of the European Union (the "Charter"). [22] Privacy principles mandated by the GDPR are analogously discussed in the U.S. Federal Trade Commission Fair Information Practice Principles ("FIPPs"), suggesting practices to prevent misuse, such as accountability and auditing, data minimization, and data security.[23] Among these fundamental rights is the right to "protection of personal data."[24] Personal data or Personally Identifiable Information is defined by the GDPR as information directly or indirectly relating to an identifiable natural person by reference to an identifier such as a name, online identifier, or other combination of factors specific to a particular user. [25] Expanded by the GDPR, the Charter's designated right of protection applies to four broad categories: individual rights, consumer control over personal information, information lifecycles, and corporate-side data privacy management procedures.[26] The following Section will explore these protections and analyze how consumers and businesses interact under the GDPR.

A. What Rights Does the GDPR Afford to Consumers?

---

[21] *See* SeeUnity, *The Main Differences Between the DPD and the GDPR and How to Address Those Moving Forward*, BRITISH LEGAL TECH. FORUM (Feb. 2017), https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf ("Under the Directive, the amount of administrative penalties was left up to the Member States. Usually, those fines would be small and were very rarely applied. Under the GDPR, penalties [are] mandatory and uniform over all the EU States.").

[22] Charter of Fundamental Rights of the European Union, Oct. 26, 2012, 2012/C 326/02.

[23] *See* Memorandum from Hugo Teufel III, Chief Privacy Officer, Dep't of Homeland Sec. (Dec. 29, 2008), (on file with Department of Homeland Security) https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[24] European Commission, *supra* note 22.

[25] GDPR, art. 4(1).

[26] PETER SWIRE & DEBRAE KENNEDY-MAYO, U.S. PRIVATE-SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS 21 (Julia Homer ed., 2d ed. 2018).

Expansive in reach, the GDPR protects all "natural persons,"[27] regardless of their nationality or place of residence.[28] It requires two important messages to be communicated to data subjects. First, the drafters intend for data subjects to be adequately and reliably informed of EU fundamental freedoms and specific rights under the GDPR. Second, the EU Commission distinguishes between data "controllers" and "processors" to provide clarity with respect to whom consumers should request information from pursuant to their rights.

Entity types that use data are labeled as "controllers" or "processors," depending on their interaction with consumer personal data. A data "controller" determines the purposes and means of processing personal data.[29] In contrast, a data "processor" merely processes personal data on behalf of a controller, and does not use the data for other purposes.[30] For example, a job-search company, Indeed, collects a significant amount of personal information submitted by consumers using the service to ultimately help them find jobs.[31] Indeed is therefore a data controller, because they determine how to best use submitted consumer personal information to help provide a service: finding jobs. At the same time, a third-party entity that provides a business-to-business cloud storage service may be hired by Indeed to store consumer personal information. The cloud storage company does not have any part in determining what the data is used for, and only "processes" the data by storing it.

The rights afforded to data subjects under the GDPR reflect a two-sided approach by regulators to ensure that entities adequately protect consumers' personal data, while also indirectly providing some control over the data to consumers. The right of access permits data subjects to request information concerning personal data processed by the controller, as well as information concerning

---

[27] GDPR, art. 4(1).

[28] GDPR, rec. 2.

[29] GDPR, art. 4(7).

[30] GDPR, art. 4(8).

[31] *See* Indeed, *Welcome to the HR Tech Privacy Center*, HR TECH PRIVACY, https://hrtechprivacy.com/ (last visited Mar. 27, 2020).

profiling or other automated decision-making processes.[32] The information must also be provided in a structured, commonly used and machine-readable format, pursuant to the right to data portability.[33] The right to restriction of processing allows consumers to object to and restrict the automated processing of their personal information.[34] The right of erasure, or "right to be forgotten," permits data subjects to request that a controller erase any and all of their personal data that is stored and processed by the controller.[35]

Given the complexity of software and other technology-related services, a single service sold by a single company may require the processing of a customer's personal data by a number of third parties. This is the distinction between "controllers" and "processors." A controller is an entity that determines the purposes and means of processing personal data.[36] They are generally the product or service provider the consumer purchases from. In contrast, a processor solely does something with the personal data on behalf of the controller.[37] Businesses that qualify as processors must implement protection measures and be able to justify processing consumer personal data by being either (1) bound by a contract that sufficiently describes the restrictions placed on processors, (2) authorized to do so by other European law, or (3) given permission to do so pursuant to the data subject's explicit consent.[38]

The standard for converting identifying data into anonymous data is stringent,[39] and the GDPR encourages mitigating the risk of data breaches instead by "pseudonymizing" personal data. Pseudonymization is a process for de-identifying data, such that it cannot be linked back to the individual it pertains to. The de-identification standard of pseudonymization is met when the

---

[32] GDPR, art. 15(1).
[33] GDPR, art. 20.
[34] GDPR, art. 18; GDPR, rec. 67.
[35] GDPR, art. 17.
[36] GDPR, art. 4(7).
[37] GDPR, art. 4(8).
[38] GDPR, art. 28 (1, 3).
[39] GDPR, rec. 26 ("The [GDPR] . . . [does] not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.").

"[processed] data can no longer be attributed to a specific data subject without the use of additional information."[40] The additional information, when matched with consumer data, can identify a specific data subject.[41] Companies seeking to reduce GDPR compliance costs by pseudonymizing personal data must keep the identifying data separate and take reasonable efforts to keep those data tables secure.[42] Encryption of the identifying data is generally considered to be a reasonable effort. Only authorized persons within the same controller entity should have access to the additional information necessary to re-identify data.[43] So long as these protections are met, the pseudonymized data is exempt from the GDPR.

Companies have incentives to separate data from direct identifiers so that re-identification is not possible without reference to additional, separately stored information.[44] Psuedonymizing data may allow controllers to improve their businesses. Firstly, controllers that pseudonymize personal data have greater flexibility to utilize and analyze the data for broader purposes.[45] Specifically, controllers must collect data only for "specified, explicit, and legitimate purposes."[46] The GDPR further requires companies to follow a "purpose limitation principle," in which data can only be further processed for purposes "compatible" with specified, explicit, and legitimate purposes.[47] When considering whether a purpose is compatible with the initial intent for processing depends in part on whether appropriate safeguards exist, specifically including pseudonymization.[48] Companies may be able to realize additional revenue streams by processing data for expanded purposes if they adequately protect it with pseudonymization techniques.

---

[40] GDPR, art. 4(5).

[41] *Id.*

[42] *Id.*

[43] GDPR, rec. 29.

[44] *Id.*

[45] Gabe Maldoff, *Top 10 Operational Impacts of the GDPR: Pseudonymization*, IAPP NEWS (Feb. 12, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/.

[46] GDPR, art. 5(1)(b).

[47] *Id.*

[48] GDPR, art. 6(4)(e).

Standardized encryption methods and data protection measures align with the GDPR principles by ensuring a high level of data protection despite an increased exchange of data.[49] In doing so, businesses are guided by the GDPR to implement "Privacy by Design," data protection measures from collection to deletion.[50] Privacy by Design is a major regulatory theme in the GDPR, encouraging businesses to protect data at every stage of its use and transfer journey.[51]

Businesses can further protect consumer rights by limiting processing only to data that are adequate, relevant, and limited to the purposes the data are processed for.[52] The GDPR provides for some flexibility in implementing Privacy by Design, particularly allowing consideration of the (1) state of the art; (2) the cost of implementation; and (3) the nature, scope, context, and purposes of processing when determining the proportion of resources to allocate towards implementation.[53] Industry leaders, such as the IT Security Association Germany ("TeleTrusT"), may provide guidance with respect to the "state of the art" for particular industries.[54] A certification mechanism allows companies to demonstrate overall compliance with GDPR principles,[55] potentially boosting consumer opinion of the company. Certified companies may display appropriate data protection seals and marks on their website so consumers can easily recognize reputable businesses adhering to an independent privacy standards.[56] Businesses should consider obtaining certifications to establish trust with consumers who are increasingly educated about their privacy rights.

---

[49] GDPR, rec. 6.

[50] *See* Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, PRIVACY BY DESIGN, (Jan. 2011), https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

[51] GDPR, art. 25.

[52] *Id.*

[53] *Id.*

[54] *See generally*, *What is "State of the Art" in IT Security?*, EUR. UNION AGENCY FOR CYBERSECURITY (Feb. 7, 2019) https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security.

[55] GDPR, art. 42(1).

[56] *Id.*

B. Transparency and Education Concerning Data Practices

Consumers want knowledge and control over how their data is used.[57] Data is effectively a new form of currency, and consumers who are aware of the value of their personal data are more likely to pursue remedies addressing concerns they have over how their data is used, and to ensure that effective protection measures are established.[58] As such, educating and informing the public is key to creating a population that is knowledgeable of their privacy rights and that holds private entities accountable for their obligation to protect and minimize use of consumer data. The GDPR directly addresses the issue of who must provide information to consumers, but lacks clarity with respect to exactly how companies should inform their customers. Despite guiding clarifications, there remains much work to be done to promote consumer awareness and activism.[59]

Regarding the scope of consumers protected under the GDPR, any natural person falls under its definition, applying so long as (1) the processing took place in the context of a business within the Union, or (2) the consumer whose personal data is processed is within the Union.[60] The first scenario protects a hypothetical Colombian individual whose data is processed pursuant to a service agreement with a company processing the data within the EU (usually also located in the EU), regardless of the Colombian citizen's actual physical location, and despite the fact that Colombia

---

[57] *See e.g.,* Jo Fischl, *GDPR - It's What the Public Want: Even for Charities*, NFPSYNERGY (Aug. 16, 2017), https://nfpsynergy.net/blog/charity-gdpr-what-do-public-think.

[58] *See* Robert Waitman, *Maximizing the Value of Your Data Privacy Investments*, CISCO (Jan. 24, 2019), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf ("[D]ue to consumers' privacy concerns . . . 87% of [companies] . . . have sales delays . . . likely due to increased privacy awareness.").

[59] *See generally*, Lizzie Davey, *How Concerned are Consumers Really When It Comes to Data Privacy?*, MEDIUM (Aug. 28, 2018), https://medium.com/@AxelUnlimited/how-concerned-are-consumers-really-when-it-comes-to-data-privacy-21c4587ddc5c.

[60] GDPR, art. 3(1,2).

is not an EU member state. Non-EU residents present in the EU are protected by the GDPR.[61] The second scenario would protect the same individual if they were physically present in the Union when they submitted their personal data for processing, regardless of where the processing company operates.[62] To clarify, it is not relevant that the processing itself is done with equipment situated within the EU, nor that the establishment itself contributes to the processing, but that either the controller or data subject are within the EU. This interpretation of controllers retains liability for the improper processing of personal data of individuals physically within the EU, even if the data processor is using the data in a non-EU jurisdiction. This is reflective of and consistent with the *Google Spain* EU Commission enforcement decision, distinguishing controllers and processors as defined in Directive 95/46/EC in the context of search engines.[63]

A series of major data breaches expanded consumer awareness of data privacy, profiling, and targeted advertising, bringing the GDPR to the public spotlight. Following the illicit harvesting of Facebook user personal data by Cambridge Analytica, consumers and private parties alike called for legislators to promulgate clearer legislation and comprehensive regulation of technology companies' use of personal data.[64] At this point, consumers were already receptive to comprehensive privacy legislation such as the GDPR, which could have helped to guide companies and prevent data breaches that resulted in lost consumer trust. A notable problem in this area concerns the lack of clarity companies give consumers as

---

[61] *Id.*

[62] *Id.* Anyone located in an EU member state is covered; protections apply based on location at the time of data submission, and not timing of the use of the data with relation to the consumer's location.

[63] Case C-131/12, Google Spain SL v. Spanish Data Protection Agency (AEPD), 2014 E.C.R. 317 (holding that Google Spain must follow object or erasure requests from a Spanish citizen, despite the fact that the processing of the data subject's data is done outside of the EU, because Google Spain is a controller operating within the EU pursuant the Directive.).

[64] Letter from Business Roundtable, to Leader McConnell, Majority Leader of the U.S. Senate, (Sept. 10, 2019), https://s3.amazonaws.com/brt.org/BRT-CEOLetteronPrivacy-2.pdf. The Business Roundtable Letter is an open letter by 51 major technology company executives urging legislators to draft a federal consumer privacy law.

to how personal data is processed. In addition, increasingly sophisticated technological products and services introduce new risks, such as heightened profiling capabilities, which necessitate both public and private-sector cooperation to codify privacy standards. Further collaboration is necessary for regulatory bodies to provide guidance to various technology companies. Successful cooperation may lead to both heightened business efficiencies, as well as heightened protection of consumer data. Overall, the GDPR functions as a comprehensive legal mechanism that defines how and when controllers must deliver relevant disclosures to consumers and make responsible use of data and data collection.

The GDPR emphasizes educating consumers about their privacy rights, and requires companies processing data to follow certain information disclosure obligations. This success is reflected both by a dramatic increase in GDPR-related complaints, as well as significant coverage in the media.[65] Important to educating consumers about their data privacy rights are two controller obligations: the "principle of transparency," and the "information obligation."[66] Properly applying the principle of transparency to inform and educate consumers contributes to data subjects being cognizant of their rights under GDPR, allowing them to better respond to situations in which those rights could potentially have been breached. The principle of transparency guides privacy professionals with respect to how companies should best convey public facing information and disclosures.[67] This principle emphasizes that information is best conveyed concisely, and when directing information to the public, it should be easy to understand.[68] Specifically, complex technical situations must be described in such a manner that a reasonable data subject can understand, with relative ease, both the purposes for which their personal data is collected and processed, as well as who processes their data.[69] As a result,

---

[65] *See GDPR in Numbers*, EU COMM'N (May 25, 2019), https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf.

[66] GDPR, rec. 58.

[67] *Id.*; *see also* GDPR, art. 12.

[68] GDPR, rec. 58.

[69] *Id.*

consumers should ideally be more informed and educated with respect to how companies process their personal data.

The "information obligation" clarifies to controllers the situations in which information concerning the processing of consumers' personal data should be conveyed to satisfy the principle of transparency.[70] It requires that controllers provide data subjects with any information necessary to processing following the principle of transparency.[71] Data subjects should also be informed about profiling, whether they are obliged to provide personal data in specific situations, and consequences if the consumer doesn't provide it.[72]

C. Consumer Notice and Consent

In order to successfully inform and educate consumers about their relevant rights and protections, the GDPR stipulates requirements controllers must follow concerning notice and informed consent from consumers pertaining to collecting personal data for processing.[73] Notice requirements mandate that controllers must adequately inform consumers about when and for what purposes their data is being processed when collecting personal data. [74] Adequate consent requires a clear affirmative act establishing an *informed* indication of the data subject's given agreement.[75] A declaration of consent must use clear and plain language, and unfair terms should not be included.[76]

The scope of consent and notice requirements under the GDPR has been subject to extensive debate and still requires further clarification by regulators. National privacy regulators provide guidance for GDPR interpretation and work with the EU to enforce GDPR violations and determine appropriate safeguards.[77] Pursuant

---

[70] GDPR, rec. 60.
[71] *Id.*
[72] *Id.*
[73] GDPR, rec. 42.
[74] GDPR, art. 13.
[75] GDPR, rec. 32.
[76] GDPR, rec. 42.
[77] GDPR, rec. 102.

to its first GDPR enforcement action, French privacy regulators released a strict interpretation of GDPR defined terms, namely "adequate notice" and "valid consent," and clarified that notice provided must be clear and easy for consumers to find.[78] In a published enforcement decision, the Commission nationale de l'informatique et des libertés (the "CNIL") denounced Google's use of consumers' personal information, specifically stating that Google violated the obligations of transparency, provided inadequate information, and lacked valid consent.[79] The judgement resulted in a fine of 50 million euros.[80] In observance of Google's noncompliance with GDPR notice requirements, the CNIL addressed the structure of data processing notices, criticizing the provided information as incomplete, "disseminated across several documents," and unduly "generic and vague."[81] According to the CNIL, users were unable to "fully understand the extent of processing operations."[82] The regulatory body's opinion also stressed the importance of providing notice to users in a manner that ensures, with a reasonable degree of certainty, that consumers will actually read *and* understand the contents of the GDPR privacy disclosures provided to them.[83] In sum, the CNIL's guidance clarified that the GDPR notice and consent mandates require more than simply providing data upon request, but also require adequate consolidation of disclosures into a single or few short, concise, and informative written documents.[84]

The CNIL decision is binding only on matters related to France because the GDPR is enforced by individual nations;[85] Google is therefore liable in this case to France and its relevant consumers. The CNIL report serves as guidance for private parties to work with

---

[78] *See The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE LLC*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] GDPR, art. 50.

regulatory groups in creating privacy programs. As France's guidance doesn't have a bearing on another country's enforcement decisions, there is a potential for enforcement inconsistencies among member states, despite consistent terminology in drafted laws.

D. Private Investment in Data Privacy

Businesses, now more than ever, are required to concern themselves with legal compliance requirements, especially with respect to developing internal programs for data protection. The increased importance of data protection has led data subjects to expect reasonable notice of and control over the processing of their personal data.[86] It also created value in developing GDPR-compliant data protection programs, potentially resulting in profits derived from efficiencies and cost reductions to implementing companies.[87] Realistically, the sheer number of GDPR-related complaints filed with data protection authorities, coupled with the risk of regulator enforcement penalties, provides justification for businesses to develop GDPR-compliant privacy programs.

Businesses acting to address privacy concerns begin by establishing a core privacy team. Central to the successful development of a privacy protection strategy is the appointment of an effective Data Protection Officer ("DPO"). The GDPR requires companies to appoint a DPO in certain situations, such as if the company's core activities consist of processing consumer data.[88] DPOs inform and advise companies of their applicable obligations under the GDPR. Generally, DPOs have legal and data analytics training, but can be diverse in background and thereby resourceful

---

[86] *GDPR One Year Anniversary: Hundreds of Thousands of Cases - And the DPOs to Handle Them*, INT'L ASS'N OF PRIVACY PROF'LS, https://iapp.org/media/pdf/resource_center/GDPR_Anniversary_Infographic_2019.pdf (last visited Dec. 12, 2019).

[87] Sara Merken & Daniel R. Stroller, *Privacy Rises in M&A Playbook as New Laws Highlight Risks*, BLOOMBERG LAW (Jan. 31, 2019), https://news.bloomberglaw.com/privacy-and-data-security/privacy-rises-in-m-a-playbook-as-new-laws-highlight-risks.

[88] GDPR, art. 37(1)(b).

when advising internal groups.[89] Importantly, a DPO cooperates with and provides a default point of contact for regulatory agencies to discuss compliance or other issues related to data processing activities.[90] Although the GDPR only requires a DPO for specific situations, companies that process consumer personal data nonetheless should consider appointing a DPO for general internal data privacy purposes to assist in communication both with regulatory bodies and internal software developers to best implement data protection strategies.

Private investment in privacy programs has resulted in tangible business benefits following GDPR implementation.[91] Businesses continue to invest significant resources in reaching GDPR compliance, costing the vast majority of affected companies more than $1M to prepare.[92] Despite this, the value-add in GDPR compliance is clear: Companies that are GDPR-compliant have a competitive advantage due to organizational efficiencies and enhanced brand value.[93] Also, due to data minimization requirements under the GDPR, businesses must remove redundant or unneeded data, which leads to efficiency savings such as faster data migration, lower storage costs, and reduced costs associated with data requests.[94] Companies with actively managed programs are generally superior in quickly addressing data losses or breaches, as well as other privacy issues.[95] Companies should seek legal and technical advice to consider options for preventing long-term costs

---

[89] GDPR, art. 39(1)(a).

[90] GDPR, art. 39(1)(d, e).

[91] *Cisco 2019 Data Privacy Benchmark Study Shows Organizations Gaining Business Benefits from Data Privacy Investments,* CISCO (Jan. 24, 2019), https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1963564. [hereinafter *Cisco 2019*].

[92] *Pulse Survey: GDPR Budgets Top $10 Million for 40% of Surveyed Companies*, PWC, https://www.pwc.com/us/en/services/consulting/library/general-data-protection-regulation-gdpr-budgets.html. (last visited Mar. 7, 2020).

[93] *Cisco 2019*, *supra* note 91 (GDPR compliance cost eighty-eight percent of affected companies more than $1M).

[94] David Kemp, *The GDPR Paradox: How Data Regulation Creates Revenue Streams*, TECHRADAR (Feb. 14, 2019), https://www.techradar.com/news/the-gdpr-paradox-how-data-regulation-creates-revenue-streams.

[95] *Cisco 2019*, *supra* note 91.

associated with data use inefficiencies, consumer complaints, and data breaches, as well as in helping implement a core privacy program.

Lacking a privacy protection core compliant with the GDPR has direct opportunity costs, evidenced by the fact that many companies experience delays in sales due to consumers' requests related to data privacy. [96] Implementing standards and automated privacy programs is the best way to directly address developing consumer concern for the protection of their privacy. Avoiding the GDPR data protection requirements is no longer an option for companies that process personal data because several jurisdictions, including states within the U.S., have drafted new privacy laws structured with the GDPR as a baseline model.[97] Successful consumer education and awareness, as well as increased investment in privacy core programs, is key to the long-term development of effective programs protecting consumers' privacy. Data protection rights under GDPR are no longer a suggestion for companies to follow if they wish to do business in the EU; compliance is now a prerequisite.

II. U.S. STATE PRIVACY LAW EMERGENCE

The drafters of the GDPR intended for the regulation to harmonize the protection of defined fundamental rights and to ensure the free flow of personal data across international borders.[98] In doing so, the GDPR has significant extraterritorial application in its enforcement. [99] Specifically, the regulation applies when companies, regardless of their establishment in the EU, process the personal data of data subjects physically present in the EU. [100] Technology companies in the U.S. initially felt regulatory pressure

---

[96] *Maximizing the Value of Your Data Privacy Investments: Data Privacy Benchmark Study*, CISCO (Jan. 24, 2019), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf.

[97] *See, e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2018).

[98] GDPR, rec. 3.

[99] GDPR, art. 3(2).

[100] *Id.*

to comply with GDPR provisions, such as consent policies, even before state governments followed in developing new privacy laws.[101] As such, businesses weren't entirely caught off guard when states introduced new laws regulating the use of consumer data.[102] Notably, California promulgated the California Consumer Privacy Act as the first statewide, comprehensive privacy law in the U.S., containing many elements similar to the GDPR.[103] Later, Washington State released the a draft bill of the Washington Privacy Act in early 2019.[104] The California and Washington bills provide for many consumer rights found in the GDPR. The bills also focuses on tailoring privacy laws to encompass emerging, complex technologies, while ensuring adequate specificity in providing regulatory guidance to affected companies.

A. The California Consumer Privacy Act

The California Consumer Privacy Act (the "CCPA") commenced enforcement on January 1, 2020.[105] The CCPA is the first of comprehensive state privacy laws, and will be enforced by the California Attorney General by July 1, 2020.[106] The CCPA

---

[101] Caroline Spiezio, *Google's GDPR Fine is a Warning for Tech Company GCs: Double Check on Data Consent Policies*, LAW.COM (Jan. 23, 2019), https://www.law.com/corpcounsel/2019/01/23/googles-gdpr-fine-is-a-warning-for-tech-company-gcs-double-check-data-consent-policies/.

[102] *See* Piotr Foitzik, *How to Make Your GDPR and CCPA Data-Management Operational*, INT'L ASS'N OF PRIVACY PROF'LS (Jan. 28, 2020), https://iapp.org/news/a/how-to-make-your-gdpr-and-ccpa-data-management-operational/.

[103] *See* Kurt R. Hunt & Leanthony D. Edwards, Jr., *CCPA: The 1st Major American Foray into Comprehensive Data Privacy Regulation*, THE NAT'L L. REV., (Dec. 19, 2019) https://www.natlawreview.com/article/ccpa-1st-major-american-foray-comprehensive-data-privacy-regulation.

[104] *See* Monica Nickelsburg, *Washington State Considers New Privacy Law to Regulate Data Collection and Facial Recognition Tech*, GEEKWIRE (Jan. 22, 2019), https://www.geekwire.com/2019/washington-state-considers-new-privacy-law-regulate-data-collection-facial-recognition-tech/.

[105] *See* California Dep't of Justice, California Consumer Privacy Act (CCPA) Fact Sheet, https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf.

[106] CAL. CIV. CODE § 1798.185(c) (West 2018).

empowers Californians to make data access requests from product and service providers.[107] Importantly, the CCPA opened the gates for comprehensive privacy legislation among U.S. states. Despite being a first-mover and providing a platform for other states to draft comprehensive privacy laws, the circumstances around the CCPA's introduction led to a flawed draft bill.[108] The CCPA has since required significant and continued clarification, resulting in revisions redlined by the AG and DOJ.[109] It has also been criticized for being expensive for companies to implement. An economic impact assessment prepared for the AG found that combined organizational spending may total $55 billion to achieve initial compliance with the CCPA.[110] Despite the potential for high implementation costs, the CCPA and similar emerging legislation may result in increased efficiencies for companies utilizing automation and better organizing data.[111] As a result of the CCPA and similar laws' expansive enforcement reach, the sheer number of companies implicated has opened markets for compliance tools created by data privacy experts, some of which utilize AI capabilities to efficiently address business data privacy obligations.[112] The rise of private use of automated legal services to

---

[107] *Id.*

[108] Melanie Mason, *Heading Off a Ballot Fight, California Lawmakers Approve Consumer Privacy Rules*, L.A. TIMES (June 28, 2018), https://civicas.net/news-blog/2018/7/3/heading-off-a-ballot-fight-california-lawmakers-approve-consumer-privacy-rules.

[109] Text of Modified Regulations, Title 11, Div. 1, Ch. 20, California Consumer Privacy Act (Mar. 11, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-second-set-mod-031120.pdf.

[110] BERKELEY ECONOMIC ADVISING AND RESEARCH, LLC, STANDARDIZED REGULATORY IMPACT ASSESSMENT: CALIFORNIA CONSUMER PRIVACY ACT OF 2018 REGULATIONS (Aug. 2019), http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

[111] Ken Briodagh, *Companies Using AI and IoT Together Have Advantage, Study Says*, IOT EVOLUTION (Nov. 4, 2019), https://www.iotevolutionworld.com/iot/articles/443637-companies-using-ai-iot-together-have-advantage-study.htm. (Implementation of Internet of Things and AI together result in "decreased costs or expenses (85 percent), improved employee productivity (87 percent), [and] streamlined operations (86 percent).").

[112] *See, e.g., About SixFifty*, SIXFIFTY, https://www.sixfifty.com/about/. (last

comply with the CCPA and related privacy laws will predictably result in lowered costs to achieve heightened efficiencies from organized data as companies see the positive investment value in utilizing automated services for internal data privacy programs.

The CCPA represents the continuation of the GDPR era of data privacy regulation. Similar to the GDPR, the CCPA's enforcement reach is expansive. Any business that collects personal information about California residents falls within the regulatory scope of the CCPA.[113] Personal information is defined consistently with current California data breach notification requirements,[114] and excludes encrypted data from the definition of personal information.[115] Under the CCPA, consumers have rights to request details from businesses concerning their personal information.[116] These access rights are similar to the "Right of Access" under the GDPR, and require businesses to disclose the sources and types of personal information collected, as well as the business purposes for collecting or selling the information.[117] Businesses must also return copies of consumer information describing the categories of third parties the business shares personal information with.[118]

Consumers find security in being able to have their personal information deleted; California residents enjoy the right to request a business to delete any personal information about the consumer that the business has collected from the consumer.[119] This provision is comparable to the GDPR "Right of Erasure." The CCPA limits this provision by providing for circumstances in which businesses do not have to comply with consumer requests.[120] Examples include completing a transaction related to the personal information, detecting security incidents, debugging, exercising free speech, research, internal uses aligned with reasonable consumer

---

visited Mar. 7, 2020) (Sixfifty is a company that provides AI-backed legal services for compliance with California and Nevada's data privacy laws.).

[113] CAL. CIV. CODE § 1798.140(g) (West 2018).

[114] *Id.* § 1798.140(o)(1).

[115] *See* Assemb. B. 1355 § (4) (Cal. 2018).

[116] CAL. CIV. CODE § 1798.110 (West 2018).

[117] *Id.* § 1798.110(a)(1-3, 5).

[118] *Id.* § 1798.110(a)(4).

[119] *Id.* § 1798.105(a).

[120] *Id.* § 1798.105(d).

expectations, and compliance requirements related to other laws.[121] Of note, the CCPA allows businesses to not comply with delete requests if the business finds it necessary to retain personal information to "use the personal information, internally, in a lawful manner which is compatible with the context in which the consumer provided the information."[122] This provision, if interpreted broadly by courts, would seemingly provide significant flexibility to companies in denying user requests to delete personal information. Companies affected by the CCPA should consider implementing automated functionality when accommodating data delete requests.[123] Besides complying with the CCPA and increasing efficiency in addressing consumer delete requests, automated systems bolster security and decrease the risk of data breaches.

Privacy laws such as surveillance laws are often written with the goal of educating and informing consumers about options from which they can select to exercise their rights and enjoy data protection.[124] To achieve the goal of providing equal protections under the CCPA, the draft proposals incorporate by reference the Web Content Accessibility Guidelines from the World Wide Web Consortium, to provide legal backing to current industry standards for internet accessibility.[125] This is especially relevant when consumers want to restrict the use of their personal information but aren't cognizant of viable means to do so. The Cambridge-Analytica scandal is an example of a recent motivator behind the drafting of the CCPA during 2018.[126] To address the previous inability of consumers to restrict the sale of their personal data to unwanted

---

[121] *Id.* § 1798.105(d)(1-8).

[122] *Id.* § 1798.105(d)(9).

[123] *See* Neel Lukka, *CCPA, GDPR and Beyond: The Future of Data Privacy Legislation*, VALUEWALK (Jan. 24, 2020), https://www.valuewalk.com/2020/01/ccpa-gdpr-amp-data-privacy-legislation/ ("analyzing data and verifying request[s]… [is] difficult to [scale]… without significant resources").

[124] *See* COUNTY OF SANTA CLARA, CAL., CODE OF ORDINANCES § A40-1, ("The Board finds it essential to have an informed public discussion"); DAVIS, CAL., MUN. CODE § 26.07.010, ("The city council finds it essential to have an informed public debate").

[125] *See* Text of Modified Regulations, *supra* note 109.

[126] Assemb. B. 375 § 2(g) (Cal. 2018).

recipients, such as data mining firms, the CCPA requires companies to provide two or more methods of submitting requests for information.[127] Businesses commonly provide a toll-free telephone number as one form of communication for submitting relevant requests.[128]

The CCPA also requires businesses to provide a link on their website homepage that, when clicked, directs users to a "Do Not Sell My Personal Information" or "Do Not Sell My Info" link on the business' website or mobile application.[129] Displaying this link satisfies the second method for submitting requests. Further, if the business operates exclusively online and has a direct personal information collection relationship with the consumer, the consumer should only be required to submit their email address when they request data.[130] The linked "Do Not Sell My Personal Information" form must enable consumers to opt-out of the sale of their personal information by the company they provided it to.[131] The homepage link also serves as notice to consumers, informing them that the company processes consumer personal information, and that the consumer has the right to request them to stop.

The CCPA mandates that companies that receive requests to not sell personal information must not discriminate against the target consumer.[132] A company discriminates when they deny goods or services, charge different prices or rates, provide a different level of quality, or suggest that the consumer will receive any of the aforementioned business penalties.[133]

Recent modifications to the CCPA by the AG provide clarity to terms defined unclearly in prior CCPA drafts. Currently, there is significant discussion regarding the definition and scope of

---

[127] CAL. CIV. CODE § 1798.130(a)(1) (West 2018).

[128] *Id.*

[129] *Id.* § 1798.135(a)(1).

[130] *Id.*

[131] *Id.* § 1798.135.

[132] *Id.* § 1798.125(a)(1); *see also* § 1798.135(c) ("A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf.").

[133] CAL. CIV. CODE § 1798.125(a)(1)(A-D).

"personal information" under the CCPA. Personal information is defined to include information that identifies, is capable of being associated with, or could reasonably be linked with a particular consumer or household.[134] The definition of "sale" is overbroad and applicable outside of the traditional definition of sale.[135] Under the CCPA, transferring consumer personal information for monetary or other valuable consideration constitutes a "sale." Pursuant to this definition, a transfer of rights to a third party to use data pursuant to an agreement with said third party would be a "sale." This is despite any transfer of cash; the analytics service provided is sufficiently under the meaning of "valuable consideration" related to the definition of "sale."[136]

The CCPA marks the beginning of comprehensive U.S. state privacy laws post-GDPR. It differs from GDPR in several respects. The CCPA utilizes different terminology, has a more expansive definition of personal information, and requires companies to add a "Do Not Sell My Personal Information" link to their homepage. Despite its difference, the CCPA is largely similar to the GDPR in providing control to consumers over the processing of their personal data. The CCPA will likely provide a foundation for other state privacy laws.

B. The Washington Privacy Act

The Washington Privacy Act ("WPA") is a new comprehensive privacy bill introduced by state legislators following the GDPR. The WPA contains elements present in the GDPR, and also addresses privacy concerns surrounding emerging technologies. Although the bill in its first draft failed to pass, its framework provides insight into the direction that jurisdictions in the U.S. are moving with respect

---

[134] *Id.* § 1798.140 (o)(1).

[135] CAL. CIV. CODE § 1798.140(t) ("'Sell,' 'selling,' 'sale,' or 'sold,' means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.").

[136] *Id.*

to data privacy laws. The WPA has since been re-drafted, with an expanded emphasis on regulating facial recognition technology.[137]

The reach of the WPA is narrower than the GDPR and CCPA in scope. A "consumer" protected by the Act is defined as a Washington resident acting only in an individual or household context.[138] The WPA also uses a narrower definition of "personal data" than the CCPA: "any information that is linked or reasonably linked to an identified or identifiable natural person."[139] Put together, these two definitions mean that non-Washington companies are potentially liable for improperly processing the personal data of Washington residents, even if those residents aren't currently physically located in Washington. Despite this, the state AG has exclusive enforcement power over violators of the WPA;[140] there is no private right of action built into the bill that would allow consumers to seek enforcement themselves. Interestingly, the WPA builds into the state treasury a "Consumer Privacy Account," to which civil penalties under the WPA will be deposited, for the purpose of furthering interests of the office of privacy and data protection.[141]

The WPA requires data controllers to facilitate seven "consumer rights," similar to GDPR principles.[142] Controllers have the obligation to honor the consumers' right to delete personal data concerning themselves.[143]

Another WPA provision similar to the GDPR is the right to opt-out of the processing of personal data.[144] The WPA gives consumers

---

[137] S.B. 5376, 66th Leg., Reg. Sess. (Wash. 2020).

[138] *Id*. § 3(6) ("[The WPA] does not include a natural person acting in a commercial or employment context.").

[139] *Id.* § 3(25)(a) ("'Personal data' does not include deidentified data or publicly available information").

[140] *Id.*

[141] *Id.* § 13 ("All receipts from the imposition of civil penalties… must be deposited into the [Consumer Privacy] account...[and] may only be used for the purposes of the office of privacy and data protection.").

[142] *Id.* § 6 The seven rights include the rights of: (1) access; (2) correction; (3) deletion; (4) data portability; (5) opt-out; (6) responding to consumer requests; and (7) establishing a consumer appeal process.

[143] *Id.* § 6(3).

[144] *Id.* § 6(5). ("A consumer has the right to opt out of the processing of personal data concerning such consumer for purposes of targeted advertising, the

the right to opt-out of profiling activities which produce "legal effects concerning a consumer." [145] This demonstrates the Washington State legislature's intent to shape new privacy laws to address sensitive issues of public policy resulting from rapidly improving profiling techniques in the context of emerging technologies.

The WPA is unique in that it specifically regulates the use of emerging technologies, with a special focus on consent and transparency in the context of facial recognition technologies.[146] It requires controllers using facial recognition for profiling to obtain consent from consumers and "employ meaningful human review" before making decisions that produce legal effects on consumers.[147] The WPA also requires processors to hire independent contractors to test facial recognition services and verify accuracy of results.[148] Particularly, processor facial recognition services must not result in unfair performance across different categories of "race, skin tone, ethnicity, gender, age, or disability status."[149]

The WPA also requires privacy teams to make "data protection assessments" when any change in processing of user data materially impacts the risk to individuals.[150] Data protection assessments allow companies to identify and weigh the benefits of particular processing.[151] Assessments conducted must consider the type of personal data processed, as well as the context it is processed in.[152] Where risks to consumers outweigh controller interests, the controller must obtain consumer consent that is "as easy to withdraw as to give."[153]

---

sale of personal data, or profiling… that produce[s] legal effects… concerning a consumer.").

[145] *Id.* § 2(6) ("Decisions that produce legal effects… include… the denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, and access to basic necessities, such as food and water").

[146] *Id.* § 17.

[147] *Id.* § 3(21) ("'Meaningful human review" means review or oversight by [trained] . . . individuals.").

[148] *Id.*

[149] *Id.*

[150] *Id.*

[151] *Id.*

[152] *Id*.

[153] *Id.*

Though not yet enacted, the WPA as drafted represents a significant step towards states adopting comprehensive privacy legislation reflective of the GDPR. Looking forward, businesses should pay special attention to guidance released by regulatory bodies concerning new privacy legislation. The WPA particularly focuses on emerging technologies such as facial regulation, and as such, future legislation will likely converge to reflect many of the same requirements in the WPA as consumers become more cognizant of privacy concerns in the context of new and emerging technologies.

III. THIRD COUNTRIES AND ADEQUACY DECISIONS

The GDPR has inspired a number of countries to draft new data privacy laws. This is in part due to the EU Commission's designation of certain non-EU countries as secure and in adherence with EU principles of data protection, allowing data transfers to those countries with fewer barriers. As a baseline, the GDPR allows EU citizens' data to be transferred to countries outside of the EU only if the transfer is based on an adequacy decision, or if the transfer is subject to appropriate safeguards.[154] Countries that implement consumer privacy laws that are compatible with the fundamental values of the EU, that also guarantee an adequate level of protection as would be ensured within the EU, may be eligible for an adequacy decision.[155] Adequacy decisions are important for economies interested in consumer data from the EU market; data transfers based on adequacy decisions don't require implementation of extra safeguards and are therefore less burdensome for entities to perform.

Whether a country has received an adequacy decision determines under what circumstances companies within their borders can process personal data. Chiefly, the GDPR stipulates that proper processing of data occurs only if either specific authorization from a supervisory authority is given, or if "appropriate safeguards" are implemented to ensure the protection of data subject personal

[154] GDPR, art. 44.
[155] GDPR, rec. 104.

data. [156] Companies may satisfy the appropriate safeguards requirement by implementing (1) binding corporate rules ("BCRs"); or (2) by assenting to standard data protection clauses adopted or otherwise approved of by the EU Commission.[157] BCRs are internal codes of conduct addressing personal data transfers to third countries and address entities that may come in contact with the data. Specifically, members of joint economic activities involved in the processing of consumer personal data must agree to follow BCRs before transferring and processing the data. [158] Although implementing BCRs requires the approval of an appropriate supervisory authority,[159] BCRs ultimately result in efficient cross-border transfers of personal data to companies in "unsecure" third countries.[160] This is because BCRs can be standardized and written into agreements between companies to balance risk while complying with data transfer requirements. Alternatively, businesses can utilize SCCs approved by the EU Commission which govern relationships between controllers and processors. The regulator-approved clauses are generally implemented into contracts between applicable controllers and processors, but shouldn't be relied upon alone, as additional safeguards are generally recommended.[161]

Nations quickly caught on to the potential for economic advantages from a favorable adequacy decision. Data transfers to countries with adequacy decisions ("secure countries") are subject to fewer restrictions than transfers to countries outside of the EU ("third countries"). In pursuing potential adequacy decisions, nations follow the GDPR principles in implementing comprehensive laws. A select few countries outside of the EU are secure, including Argentina, Israel, and Switzerland.[162] A favorable

---

[156] GDPR, art. 46(2).

[157] GDPR, art. 46 (2)(b-d).

[158] GDPR, art. 47(1)(a).

[159] GDPR, art. 47(1).

[160] GDPR, art. 46. Appropriate safeguards for transfers such as Binding Corporate Rules are required in the absence of an EU Commission decision of adequacy concerning data transfers to a particular third country.

[161] GDPR, rec. 109.

[162] Intersoft Consulting, *GDPR Third Countries*, INTERSOFT CONSULTING, https://gdpr-info.eu/issues/third-countries/ (last visited Jan. 15, 2020).

decision could attract foreign investments in domestic technology sectors, as well as bolster economic growth as a result of domestic companies realizing efficiencies in transferring data across EU Member State borders. For example, if the UK is deemed secure by the EU Commission, it would return to unrestricted data transfers with EU member states, as after leaving the EU the UK is an unsecure third country under the GDPR.[163]

The U.S. and Canada are partially secure.[164] The GDPR allows for the EU Commission to issue partial adequacy decisions. Specific to U.S. companies, recipients of EU consumer data must belong to the Privacy Shield, a framework that provides companies a mechanism to comply with data protection requirements in cross-border transfers.[165] The Privacy Shield sufficiently bridges the gap between U.S. data treatment and requirements in the GDPR in part because it requires participating companies to designate a compliance third party, allowing for direct interaction between U.S. companies and regulators.

The GDPR sets out requirements for transferring EU resident data to third countries. The first requirement is that the data transfer itself is authorized by consent, contract, or the protection of vital interests.[166] Supposing the transfer is legal the next step is to consider whether the country is secure or unsecure.[167] Secure third countries confirm a "suitable level of data protection with national laws" that are comparable to the GDPR.[168] Data transfers to such countries are expressly permitted.[169] Costs associated with

---

[163] Michael Thompson & Paul Hughes, *Brexit: How Do US and Overseas Investors Take Advantage?*, STEPTOE (Sept. 27, 2019), https://www.steptoe.com/en/news-publications/brexit-how-do-us-and-overseas-investors-take-advantage.html.

[164] *See generally*, *International Transfers*, INFO. COMM'R OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/ (Last visited Jan. 20, 2020).

[165] *Privacy Shield Program*, PRIVACY SHIELD FRAMEWORK, (Jul. 12, 2016), https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1.

[166] Intersoft Consulting, *supra* note 162.

[167] *Id.*

[168] *Id*.

[169] *Id.*

subjecting domestic companies to new privacy laws are balanced by potential economic opportunity from the free flow of data that would move across the secure country's borders, leading to a potentially expanded presence in European markets, as well as to foreign investment within the secure country itself.

Appropriate safeguards for transfers to third countries include legally binding and enforceable contracts, binding corporate rules, and standard protection clauses. There is some flexibility with respect to how a company implements safeguards in cross-border data transfers, allowing an "approved code of conduct" or "certification mechanism" in conjunction with binding corporate rules or other safeguard requirements, to satisfy the GDPR requirement.[170]

Notably absent from the GDPR is a specific mechanism or general requirement list from which legislators in third countries can draw guidance to construct new national privacy laws. As such, laws seeking to comply with GDPR requirements for adequacy have been drafted and approved with only foundational consistency. Following is a discussion of international jurisdictions that have drafted and approved of new privacy laws complying with the GDPR principles, as well as potential issues those laws may introduce.

A. Japan

Japan became a secure country on January 23, 2019, joining other secure countries in creating the world's largest area of safe data flows.[171] Japan's successful implementation of GDPR-compliant privacy laws may serve as a model for other third countries developing comprehensive privacy laws. The Japanese government promulgated the Act on Protection of Personal Information (the "APPI"), a comprehensive privacy law containing elements that may be used as a model for third country privacy law considerations.[172]

---

[170] *Id.*

[171] Id.

[172] Kojinjōhōnohogonikansuruhōritsu [Act on the Protection of Personal Information], Law No. 57 of 2003, translated in (Personal Information Protection Commission, Japan),

The EU Commission reached an adequacy decision based on three key elements despite narrower consumer protections found in the APPI compared with the GDPR.[173] First, the Japanese, in conjunction with the EU Commission, set out "Supplementary Rules" to reconcile differences between the two jurisdictions privacy protection laws.[174] Specifically, the Supplementary Rules reconciled ambiguities and confusion concerning the protection of sensitive data, the exercise of individual rights, and the conditions required for importing EU data into Japan.[175] Second, the Japanese government assured the EU Commission that Japan would provide minimized access of personal data to law enforcement to be used in a "necessary and proportionate" manner, subject to "independent oversight and effective redress mechanisms" for criminal and national security purposes.[176] Finally, the Japanese government implemented a compliance handling mechanism to address complaints from consumers regarding Japanese public authority access to personal data.[177]

Strong protection guarantees and the establishment of an independent data protection committee contributed to Japan's adequate level of data protection. Specifically, the EU and Japan agreed to a reciprocal recognition with respect to the adequate level of data protection.[178] This clarifies the EU Commission's criteria in evaluating third countries for adequacy decisions, in that the EU

---

https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf (Japan) [hereinafter APPI].

[173] *See* Michiro Nishi, *Data Protection in Japan to Align with GDPR*, JD SUPRA (Sept. 26, 2018), https://www.jdsupra.com/legalnews/data-protection-in-japan-to-align-with-98982/.

[174] *See* Ius Laboris, *Japan – EU Data Protection Agreement Takes Effect*, LEXOLOGY (Feb. 15, 2019), https://www.lexology.com/library/detail.aspx?g=afcfd8f8-fd19-400b-b65c-f158a6524871.

[175] Press Release, European Commission, European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows (Jan. 23, 2019) (on file with author).

[176] *Id.*

[177] *Id.*

[178] Věra Jourová, *EU Japan Adequacy Decision*, EUR. COMM'N (Jan. 2019), https://ec.europa.eu/info/sites/info/files/research_and_innovation/law_and_regulations/documents/adequacy-japan-factsheet_en_2019_1.pdf.

Commission interested in independent data supervision.[179] In ideal circumstances under GDPR, data flowing among secure countries would have no linked "nationality" with respect to treatment and protections under various applicable data privacy laws.

The establishment of the Personal Information Protection Commission (the "PPC") as an independent supervisory authority heavily supported an adequacy decision. [180] The EU Commission explains that independence sufficient for an adequacy decision requires the power to "take . . . action to bridge differences of the systems and operations" between Japan and foreign jurisdictions, but also to "establish enhanced protections through the adoption . . . of stricter rules . . . going beyond . . . the APPI."[181] The extent of independent power and regulatory flexibility given by the Japanese government to the PPC stands as one of the EU Commission's main justifications in adopting an adequacy decision for Japan, as the Commission specifically noted that the establishment of a supervisory authority brought the Japanese data protection system closer to the GDPR.[182]

In sum, Japan was able to secure a favorable adequacy decision from the EU by providing for (1) relatively strict adherence to GDPR principles in its domestic privacy laws, (2) establishing an independent regulatory body, and (3) bridging gaps between EU and Japanese data protection regulations with established "Supplemental Rules." Other jurisdictions that seek to attain an adequacy decision from the EU Commission should strive to establish a regulatory body that has independent rulemaking and enforcement powers that can adapt to external factors such as guidance from EU regulatory bodies.

B. India

Not long after the GDPR entered into effect, India released the Personal Data Protection Bill of 2018 (the "PDP"), replacing the

---

[179] GDPR, rec. 104.

[180] APPI, art. 59(1).

[181] Jourová, *supra* note 178.

[182] Commission Implementing Decision (EU), 2019 O.J. (L 76/1) (EC). https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf.

Sensitive Personal Data and Information Rules of 2011. The Indian government replaced the 2018 Bill in 2019, relaxing requirements related to localized data storage.[183] The PDP utilizes language inspired by the GDPR, with variation in terminology, such as using "data principals" instead of "data subjects."[184] The PDP is similar to other jurisdictions' privacy laws in that it has broad enforcement reach, applying to the processing of personal data in connection with business in India, or profiling of Indian data subjects.[185] Rights afforded to data principles are similar to those under the GDPR, including rights of confirmation and access, correction, data portability, and erasure.[186] Indian organizations were some of the

[183] Kurt Wimmer & Gabe Maldoff, *India Proposes Updated Personal Data Protection Bill*, INSIDE PRIVACY, (Dec. 12, 2019), https://www.insideprivacy.com/india/india-proposes-updated-personal-data-protection-bill/. The fact that India replaced its 2018 bill with a new version is significant; given the early introduction of India's draft bill in relation to the enactment of the GDPR, it is clear that the Indian government was interested in early consideration of EU regulator recognition. Specifically, a decision from the EU Commission designating India as a jurisdiction that adequately protects consumer data pursuant to the GDPR principles would greatly benefit India's rising technology economy. Data localization requirements would also increase the Indian government's ability to surveil its citizens. Together, data localization requirements weaved into a comprehensive data privacy law that otherwise conforms with the GDPR principles tests the boundaries of EU Commission decisions regarding expectations for national comprehensive privacy laws. Later, EU Commission decisions, such as a favorable decision to Japan, reduced the likelihood a broad data localization requirement could be deemed acceptable, resulting in a reduction in scope present in the 2019 bill. Though the EU Commission has not stated that data localization requirements violate the GDPR principles per se, other countries may take note that data localization is unacceptable in the consideration of the EU Commission, as India was unable to receive a favorable decision despite being an early mover in enacting legislation based on the GDPR principles. The relaxation of data localization requirements likely reflects this difficulty in obtaining an adequacy decision. It is also likely that a relaxation, without complete removal, is yet another test of the EU Commission's boundaries in making adequacy decisions.

[184] The Personal Data Protection Bill of 2019, art. 3(14) (India) https://prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf [hereinafter PDP].

[185] PDP, art. 2.

[186] *Id.* chapter VI.

first to comply with GDPR provisions, some starting as early as 2016.[187]

Although India has sought to be one of the earliest jurisdictions to promulgate GDPR-like privacy laws, they have not yet received an adequacy decision from the EU Commission. Likely a large contributing factor is the PDP's restrictions on cross-border transfers of personal data, with data localization requirements. Specifically, at least one copy of all personal data applicable to the Bill is required to be stored on a data server located within India.[188] The PDP continues by mandating a category of "critical personal data" that must only be processed in a server within Indian borders.[189] However, because the Indian government has the power to determine the scope of what constitutes "critical personal information," there is a potential for abusive surveillance practices.[190]

Although the Indian government seeks a favorable adequacy decision from the EU Commission, the data localization requirement within India's bill is likely to result in further delay or refusal. Businesses participating in the Indian technology industry suspect that data localization could help India protect the privacy of its citizens.[191] Restricting the free flow of data is against the intent of the GDPR, and is likely to result in government surveillance over the localized data. It is unlikely to result in an improvement in the protection of data from regular encryption and data minimization

---

[187] Data Security Council of India and Deloitte India, *DSCI-Deloitte GDPR Readiness Report: A Study of the Preparedness of Indian Organizations with the Requirements Mandated by GDPR*, DELOITTE (May 2018), https://www2.deloitte.com/in/en/pages/risk/articles/dsci-deloitte-gdpr-readiness-report.html.

[188] PDP, art. 40(1).

[189] *Id.* art. 40(2).

[190] Benjamin Parkin, *India Proposes First Major Data Protection Law: Controversial Bill Would Give Government Authorities Broad Powers to Access Personal Information*, FINANCIAL TIMES, (Dec. 11, 2019), https://www.ft.com/content/df6fd8d4-1bf1-11ea-9186-7348c2f183af.

[191] Siddharth Chakraborty, *Data Localisation in Theory Could Help Better Protect the Privacy of its Citizens*: *Kathy Bloomgarden*, THE ECONOMIC TIMES (Oct. 15, 2019), https://economictimes.indiatimes.com/tech/internet/data-localisation-in-theory-could-help-india-better-protect-the-privacy-of-its-citizens-kathy-bloomgarden/articleshow/71599787.cms.

practices. Instead, data localization requirements would hinder a company's ability to delete certain data, creating the possibility of a breach of that data. The Indian government's has displayed interest in monitoring localized data by their demanding companies to supply "unfettered supervisory access" to financial data.[192]

Data localization requirements may materially increase costs imposed on companies operating in India.[193] Short-term economic benefits stemming from the data localization requirement, such as local investments in building new data centers, are unlikely to persist in the long term. The overly broad data localization requirement under the PDP lacks sufficient justification. The Indian government should consider amending the PDP to eliminate the data localization provisions entirely, which will bring India closer to an adequacy decision.

C. Brazil

Brazil's proposed legislation, the *Lei Geral de Proteção de Dados* (the "LGPD"), regulates the use of personal data with principles similar to the GDPR. The law ensures individual privacy rights, and encourages economic and technological innovation

---

[192] *See* Letter from Nanda S. Dave, Chief General Manager, Reserve Bank of India, to Indian Banks (Apr. 6, 2018) (on file with the Reserve Bank of India), https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0.

[193] LEVIATHAN SECURITY GROUP, QUANTIFYING THE COST OF FORCED LOCALIZATION, (2015), https://wjlta.files.wordpress.com/2018/10/f4aab-quantifyingthecostofforcedlocalization.pdf. Local companies would experience a 30-60% increase in costs, resulting in a 0.7-1.1% drain of GDP from the overall economy. ("[Top international] public cloud providers [do not] have any datacenters inside [India], meaning that… companies intending to comply with... data localization laws must either use traditional datacenters, with the significant capital investment in hardware and periodic upgrades that implies, or non-public cloud providers that require exclusivity, business-wide licensing, non-disclosure agreements, or any of a host of other conditions. A forced data localization law, then, would force companies doing business in these countries to choose among a set of poor choices… even as the lack of geographic dispersion in backups makes it difficult to preserve business-critical data in the event of a large-scale disaster.").

through comprehensive regulation of the use of personal data.[194] The LGPD principles are similar to the GDPR, and the provisions regulate the processing of personal data in Brazil, processing in connection with providing goods or services to individuals in Brazil, and personal data collected in Brazil.[195] The definition of "personal data" in the LGPD is similar to the GDPR, encompassing "identified or identifiable natural person[s]."[196] Finally, it restricts the processing of personal information to circumstances similar to the GDPR, including consent, compliance with legal obligations, processing for research purposes, processing necessary for the execution of contracts, and when necessary to fulfill legitimate interests unless data subject rights outweigh the interests of an applicable company.[197]

Although the LGPD draft bill provided for the establishment of a Data Protection Authority in Brazil, as suggested by the GDPR, the President vetoed portions of the LGPD.[198] As stated by the GDPR, the EU commission takes into account whether an "independent supervisory authority" has been established in the relevant third country with power to ensure and enforce compliance with data protection rules.[199] On August 14, 2018, the President of Brazil sanctioned the LGPD and vetoed several important provisions that are likely necessary to receive an adequacy decision from the EU Commission.[200] Among the vetoed provisions is one

---

[194] Renato Leite Monteiro, *The New Brazilian General Data Protection Law – a Detailed Analysis*, INT'L ASS'N OF PRIVACY PROF'LS (Aug. 15, 2018), https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/.

[195] *Lei Geral de Proteção de Dados* Lei No. 13, 709, de Agosto 14, 2018, Aug. 15, 2018 (Braz.) art. 3(1-3). https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf [hereinafter LGPD].

[196] LGPD art. 5(1).

[197] *Id.* art. 7(1-3, 5, 9).

[198] Rodrigo Cantarino, Di Blasi, Parente & Associados, *Protecting Data in Brazil - A Brain without a Body*, L. BUS. RES. (Aug. 20, 2018), https://www.lexology.com/library/detail.aspx?g=cc70e47b-b065-4537-b1ad-3445ab2d2161.

[199] GDPR, art. 45(2)(b).

[200] *See* Javier Pallero & Caroyn Tackett, *Brazil President Approves Data Protection Bill – But Vetoes Key Accountability Measures* ACCESSNOW.ORG

that would establish the National Authority on Data Protection ("ANPD") in Brazil. This was primarily due to a constitutional technicality, requiring the creation of the ANPD by the President. Brazilian President Michel Temer was able to establish such a data protection authority before the end of his administration.[201] Despite these efforts, the ANPD is unlikely to pass scrutiny with regards to its independence because the ANPD is a body administratively attached to the president's office. As a result, the EU Commission will likely find that the established ANPD is not sufficiently capable of independent decision making, due to the fact that it (1) would receive direct orders from the Presidency,[202] and (2) lacks an independent budget.[203] This structure is unlike the Japanese data protection authority, which has independent regulatory power. The Brazilian government should recognize that the EU Commission issued Japan's favorable adequacy decision on grounds explicitly mentioning the independence of the Japanese data protection authority. It may be to Brazil's benefit to model the LGPD after the

---

(Aug. 16, 2018) https://www.accessnow.org/brazil-president-approves-data-protection-bill-but-vetoes-key-accountability-measures/; *see also* Indridi H. Indridason, *Executive Veto Power and Credit Claiming: Comparing the Effects of the Line-Item Veto and the Package Veto*, *Public Choice* Vol. 146, No. 3/4 (Mar. 2011), https://link.springer.com/article/10.1007/s11127-010-9595-8 ("In Brazil the president can [line-item] veto bills, articles, paragraphs, subsections, or subparts and his veto can be overridden by an absolute majority of legislators in a joint session of the chambers.").

[201] Robert Daniel-Shores, Daniel Law, *Brazil's DPA: It Isn't Over Until the Referee Whistles*, LEXOLOGY (Feb. 18, 2019), https://www.lexology.com/library/detail.aspx?g=09192bc8-2574-4b09-9503-81ecf6ea4cba.

[202] *See* Mattos Filho, Veiga Filho Marrey Jr., & Quiroga Advogados, *Guide to the Brazilian Data Protection Law*, MATTOS FILHO (July 2019), https://publicacoeswww.mattosfilho.com.br/books/pvaa/#p=1.EscritorioMidia/livretos/qr-code-lgpd/Guide%20LGPD.pdf (The decision-making independence of the ANPD from the Brazilian president is unclear, given its clear connection to the president. Being connected to the presidency is not consistent with having technical and decision-making autonomy. "The ANPD is a governmental entity with technical and decision-making autonomy. The ANPD is connected to the Cabinet of the Presidency.").

[203] *See* Bronte Cullum, *Brazil Creates Privacy Watchdog, but Fears Remain Over its Independence*, PINHEIRO NETO ADVOGADOS (Jan. 3, 2019), http://www.pinheironeto.com.br/imprensa/brazil-creates-privacy-watchdog-but-fears-remain-over-its-independence.

Japanese data protection model, and specifically allow the ANPD to have further decision-making.

It is unlikely that the LGPD as drafted and overseen by the current ANPD will sufficiently convince EU regulators that transfers of data to Brazil will be secure and consistently applied to harmonized GDPR and LGPD principles. The LGPD addresses many risks for data breaches and inadequate data protection laws in Brazil. The Brazilian government should continue to encourage their President to establish an independent data protection authority that can adequately supervise company adherence to the LGPD and GDPR. Creating such a regulatory body would not only increase the likelihood of Brazil receiving an adequacy decision, but also substantially reinforce safeguards against data breaches and data misuses by holding companies accountable to government supervision. It may not be the case that the ANPD requires regulatory power sufficient to establish laws that exceed requirements set forth by current privacy laws, but regulatory power and flexibility is prioritized by the EU Commission when considering adequacy decisions.

CONCLUSION

The GDPR formed the foundation for a new age of data privacy practices globally. Regardless of GDPR applicability, companies interacting with consumer personal information should be forward-looking in implementing data privacy protection programs, in anticipation of international and domestic privacy laws. Specifically, Privacy by Design, protection of data at every step of its transfer and processing, is crucial to a successful data protection program. Furthermore, pseudonymizing data is the preferred approach for preventing re-identification of encrypted data, due to comparatively low cost and resource required to ensure successful protection of the data from a potential breach. As data privacy laws require businesses to more aggressively protect consumers' data with automation and data organization, businesses are likely to see efficiencies and minimize costs due to breaches, benefitting business and consumers alike.

International jurisdictions are converging to reflect many of the same privacy principles in their new comprehensive laws. The EU

Commission has shown little room for flexibility with respect to adding provisions to data laws that have the potential to allow for government surveillance of consumers.

Consumers around the world are soon to realize benefits from the diverse array of technologies available to them. Developing privacy laws are a way to address concerns regarding private and governmental misuse of consumer data. Private business will need to be diligent in building privacy programs to comply with new data laws, so that consumers no longer need to choose between giving up data rights and utilizing emerging technologies.