NOW WHAT? A NEW DIRECTION FOR U.S. BUSINESSES AND LAW IN THE WAKE OF THE GENERAL DATA PROTECTION REGULATION

CLAUDIA FENDIAN*

I. INTRODUCTION

What is the General Data Protection Regulation ("GDPR"), and why does it matter? Most American individuals may not need nor care to have the answer. Objectively, they may not be wrong in thinking that it does not matter. The GDPR was designed and implemented to serve as a consumer protection regulation for European Union citizens, not American citizens. However, foreign laws, policies, and directives inevitably affect U.S. law, policy, and relations. Thus, the question must be asked: who needs to pay attention to the GDPR and what its new requirements entail? The answer: U.S. businesses.

The GDPR was passed by the Commission of the European Union in April 2016 and implemented in May 2018.[1] One of the primary purposes of the GDPR is to create more transparency for consumers with regard to the personal data they submit to companies and how that data is being stored, predominantly online.[2] It vastly expands the rights of consumers and outlines specific requirements for companies regarding how to store and process personal data, and how to make the data available to consumers.[3]

Before the implementation of the GDPR, American companies were largely unregulated regarding personal data and privacy.[4] Historically in the United States, laws and regulations in this subject area have arisen as needed.[5] When the need does arise, laws are generally enacted to target specific data. For example, the privacy of personal medical data is governed

* Class of 2020, University of Southern California Gould School of Law; B.A. Communication Studies, Northwestern University; Editor-in-Chief, *Southern California Interdisciplinary Law Journal*, Volume 29. Immense thanks to the editorial board of Volume 29 for their immaculate feedback and dedication to the editing process.

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

[2] NEW EUROPEAN GENERAL DATA PROTECTION REGULATION: A PRACTITIONER'S GUIDE ENSURING COMPLIANT CORPORATE PRACTICE 3 (Daniel Rücker & Tobias Kugler eds., 2018) [hereinafter A PRACTITIONER'S GUIDE].

[3] *See generally* General Data Protection Regulation, *supra* note 1.

[4] Brian C. Eaton, *GDPR: How Is It Different from U.S. Law & Why This Matters?*, LEXOLOGY: PRIVACY AND DATA SECURITY INSIGHT (Sept. 14, 2017), https://www.lexology.com/library/detail.aspx?g=4b2843f7-f67a-4015-bca9-96bd2fe344c9. *See Data Breach Notification: 10 Ways GDPR Differs from the US Privacy Model*, PWC (Dec. 2016), https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/gdpr-differences.html (providing examples of major changes the GDPR brings about to areas of law that, prior to the implementation of the GDPR, were either unregulated or had relatively mild requirements).

[5] Eaton, *supra* note 4.

by the Health Coverage Availability and Affordability Act of 1996 (HIPAA).[6] By contrast, the GDPR is designed to offer comprehensive and all-inclusive protection of what the European Union considers a "fundamental right" to data privacy and access, restricting companies' use, storage, and monitoring of any and all personal data submitted by or solicited from consumers.[7]

The GDPR is intended to apply to any business that services EU citizens or residents, regardless of whether it is based in the European Union.[8] Consequently, U.S. businesses are finding themselves anxious to comply with these newly-implemented standards in areas where they previously encountered limited regulations or rules.[9] There are also harsh fines on the horizon for any company beholden to the requirements of the GDPR who cannot demonstrate compliance or a concrete path to compliance, so GDPR provisions should not be ignored.[10]

While the GDPR establishes an array of new requirements and restrictions, this note will focus on four specific articles within the regulation and how the requirements set out in these articles are shaping U.S. business practices. Specifically, this note will analyze the changes to Article 15, Article 20, Article 25, and Article 30, and the resulting implications, as these four provisions arguably impose the most severe changes to U.S. businesses. This note will further seek to provide an analysis of what compliance with these provisions looks like for U.S.-based companies and consumers, as well as give an assessment of possible cost-effective approaches partially inspired by European counterparts. Achieving compliance can be both a timely and costly process, as some companies may need to make significant changes to the ways they store and process user data.[11] Next, this note will offer an analysis of the GDPR's impact on U.S. law and policy and its involvement in domestic and global litigation. Lastly, this note will explore the future of data privacy laws and regulations relating to the GDPR within the United States, offering a prediction of whether or how the laws and requirements may change, adapt, and shape business practices for years to come.

II. BACKGROUND

Before unpacking the four aforementioned articles of the GDPR, it is critical to understand the background, language, and context of the regulation itself. First: which consumers fall under the scope of the GDPR? The regulation protects not only EU citizens but also any EU residents.[12] The consequence of this language is that anyone residing in the European Union

---

[6] Health Coverage Availability and Affordability Act of 1996 (HIPAA), 104 P.L. 191, 110 Stat. 1936 (1996).

[7] Eaton, *supra* note 4.

[8] *E.g.*, Monica C. Meinert, *GDPR: These Four Letters Could Spell a Compliance Headache for Small Banks*, 110 ABA BANKING J. 30, 30–31 (2018).

[9] Lucy Handley, *US Companies Are Not Exempt from Europe's New Data Privacy Rules — and Here's What They Need to Do About It*, CNBC (Apr. 25, 2018, 5:43 AM), https://www.cnbc.com/2018/04/25/gdpr-data-privacy-rules-in-europe-and-how-they-apply-to-us-companies.html.

[10] *E.g.*, Claire Laybats & John Davies, *GDPR: Implementing the Regulations*, 35 BUS. INFO. REV. 81, 81 (2018).

[11] *E.g.*, *id.* at 82.

[12] Meinert, *supra* note 8, at 30.

is entitled to exercise the rights outlined in the GPDR and is entitled to the protections set forth in the regulation. Second: what data is considered "personal data" and thus within the scope of the regulation? The premise of the GDPR is that individuals should control any personal data stored by businesses.[13] "Personal data" is defined by the regulation as: "anything that could identify an individual (referred to as a "data subject" by the regulation), either on its own or when combined with other pieces of data."[14] Within the scope of this broad definition are typical identifiers of personal information, such as credit card information and passwords but also less obvious data, such as IP addresses and social media profile information.[15] Lastly, it is critical to understand that the drafters of the GDPR intentionally left the language and scope of most provisions quite broad with the hope that European consumers would be afforded as much protection and transparency as reasonably possible. Businesses can implement basic policies, such as maintaining and managing separate lists of suppliers, business clients, and individual customers, based on the types of contracts in place with the business, and ensuring that subcontractors who use or process consumer data are bound by the GDPR requirements as well.[16] Because businesses around the world are still exploring and understanding the regulation, they must prioritize finding cost-efficient solutions to achieve compliance, while still realizing the ultimate goal of the GDPR.

III. ANALYSIS OF GDPR ARTICLES 15, 20, 25 & 30

A. ARTICLE 15: "RIGHT OF ACCESS BY DATA SUBJECT"

Article 15 provides that consumers have the right to access their personal data stored with a company.[17] While on its face this provision creates a right for consumers, it also creates a challenge for businesses: they must have a reliable and efficient system in place in order to collect, process, and respond to consumers' inquiries about their personal data.[18] In requesting access to information, the consumer is entitled to over half a dozen elements of information, including but not limited to: the purposes for the processing; the categories of personal data concerned; the recipients or types of recipients to whom the personal data have been or will be disclosed or distributed; and the period of time for which the personal data will be stored or the criteria

---

[13] *Id*. at 31.

[14] *Id*.

[15] *Id*. The effects on many industries of this broad definition can be complex. *Id*. For example, banks that employ target-based marketing mechanisms, such as IP address monitoring, in order to market to potential customers could land within the scope of the GDPR if any of the potential customers are EU citizens or residents. *Id*.

[16] *Seven Steps for Businesses to Get Ready for the General Data Protection Regulation*, EUR. COMMISSION (2018), https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-business-7-steps_en.pdf.

[17] General Data Protection Regulation, *supra* note 1, at 43.

[18] *See A New Era for Data Protection in the EU: What Changes After May 2018*, EUR. COMMISSION 1, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf (last visited Nov. 7, 2018); *The GDPR: New Opportunities, New Obligations*, EUR. COMMISSION 1, 8–12, 17 (2018), https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf.

used to determine that period.[19] This creates an obligation for businesses to not only provide such information upon request but also have some sort of automated and efficient mechanism to answer inquiries in bulk.[20]

One possible, reasonable solution for compliance with Article 15 (also applicable to subsequent articles of the GDPR) is to create a standard form for consumers to use to submit access requests.[21] The creation of a standard and relatively consumer-friendly form accomplishes several goals: first, the consumer enjoys a structured, simplified, and straightforward data access request process and a clear understanding of what data are available; second, the business enjoys uniformity on the receiving end of such access requests; and third, a uniform inquiry system paves the way for a uniform response system and helps businesses stay organized throughout the entire access inquiry and response process.

This solution can be applied to many of the other articles of the GDPR and their respective requirements. When businesses create standardized forms that comply with the GDPR requirements, it results in less anxiety toward compliance overall. This makes sense: if the system a company has in place is already ensuring compliance, the process as a whole is likely to fit within the standards and recommendations set forth by the GDPR.

B. ARTICLE 20: "RIGHT TO DATA PORTABILITY"

Article 20 relates significantly to Article 15. This Article expands on the right granted to consumers in Article 15 by adding another layer of requirements for businesses. According to the text of the regulation, the requirements set forth in Article 20 apply only when data "processing is carried out by automated means."[22] While "automated means" is not explicitly defined within the GDPR,[23] a sufficient amount of businesses process data in a way that could likely be considered "automated" for this Article to have an impact on U.S. businesses.[24] Article 20 requires that companies provide consumers who request their personal data with a comprehensive summary of the data in a "structured, commonly used and machine-readable format."[25] In essence, this requirement translates to an obligation for any business with an automated system of processing data to have an internal system in place that can process requests for personal data, and produce a simplified yet complete, consumer-friendly rundown of the data being stored by the company.[26]

However, the right to access and portability is not a catchall right. One of the few limitations of Article 20 is that the right to obtain one's personal

---

[19] General Data Protection Regulation, *supra* note 1, at 43.

[20] See *infra* Parts III(B) and III(D) for a further discussion.

[21] *Right of Access*, INT'L COMMISSIONER'S OFF. (ICO), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/.

[22] General Data Protection Regulation, *supra* note 1, at 45.

[23] A PRACTITIONER'S GUIDE, *supra* note 2, at 144.

[24] *See* José Vega & Amy Puckett, *The Potential Effect of Data Portability Under GDPR*, LAW360 (Nov. 6, 2017, 1:12 PM), https://www.law360.com/articles/980883?utm_source=rss&utm_medium=rss&utm_campaign=articles_search.

[25] General Data Protection Regulation, *supra* note 1, at 45; A PRACTITIONER'S GUIDE, *supra* note 2, at 145.

[26] A PRACTITIONER'S GUIDE, *supra* note 2, at 145.

information being stored and processed by a company cannot subsequently adversely affect the freedom and protections of others.[27] While it is unlikely that personal information would be so commingled that there is any risk of affecting the rights of others, there are certain types of data that could be inherently connected to the data of others.[28] Access to these data would need to be monitored more carefully by companies when complying with portability rights and requests.[29]

Like Article 15, Article 20 creates yet another opportunity for businesses to create standard, comprehensible forms for consumers. A standardized form, paired with a functional, automated system, can aid businesses in avoiding the near-certain compliance headache that otherwise would accompany these requirements.

A. ARTICLE 25: "DATA PROTECTION BY DESIGN AND DEFAULT"

This provision states that companies should take necessary steps to mitigate any risks associated with these new processes of managing personal data by "implement[ing] appropriate technical and organizational measures . . . to integrate the necessary safeguards into the processing in order to meet the requirements of [the GDPR]."[30] While the language of this Article seems broad and even vague, there are important ramifications for businesses to consider. The processing technology, in its entirety, used by a business soliciting and storing user data must, by nature continuously prioritize protection and privacy of user data regardless of cost or timing. In essence, businesses cannot use the argument of financial burden to skirt around the requirements of the regulation, specifically regarding data protection.[31]

Article 25 also creates a responsibility for businesses to find cost-effective strategies of incorporating data protection requirements at the early or "design" stage of the data monitoring and storage process.[32] This seems to suggest that data privacy and protection should be incorporated into the entire life cycle of digital software.[33] This obligation would also apply to the launch of any new product or service, requiring an appropriate assessment of all risks to data protection and privacy beforehand.[34]

In this regard, enforcement will likely be difficult—how can it be verified that the maintenance of privacy of and proper care for personal data is incorporated into the very beginning of the data storage or product launch process, rather than simply as needed when an inquiry or audit arises?[35] It thus follows that one of the primary purposes of Article 25 is to simply

---

[27] Beata A. Safari, *Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection*, 47 SETON HALL L. REV. 809, 830 (2017).
[28] *Id*.
[29] *Id*.
[30] General Data Protection Regulation, *supra* note 1, at 48.
[31] A PRACTITIONER'S GUIDE, *supra* note 2, at 112.
[32] *Id*.
[33] *E.g*., Safari, *supra* note 27, at 830.
[34] Craig McAllister, *What About Small Businesses? The GDPR and Its Consequences for Small, U.S.-Based Companies*, 12 BROOK. J. CORP. FIN. & COM. L. 187, 194 (2017).
[35] Safari, *supra* note 27, at 831.

encourage businesses to streamline their technology for processing data by incorporating privacy into every stage of the mechanism, thus protecting data from the very beginning and perhaps lightening the burden of compliance with the remainder of the GDPR later in the processing cycle.[36]

However, another important concept relating to Article 25 is "data minimization." Data minimization is one of the overall themes of the GDPR and requires that the data processed and stored by businesses be limited to only that which is necessary.[37] Data minimization is integrated into Article 25, as it is required throughout the life cycle of data processing.[38] This includes: types and scope of the data collected; the length of time for which personal data may be stored; and the requirement that data be destroyed after use.[39]

The concept behind data minimization is mitigation of the risk that businesses and other data controllers might mishandle sensitive information; if there is only a minimal amount of information being stored by a business in the first place, there is less data that could potentially be leaked or misused.[40] Nonetheless, Article 25, taken in the context of data minimization, presents a serious issue for U.S. businesses. Since Article 25 requires that the entire process of receipt, storage, and disposal of consumer data incorporate privacy and data protection "as part of the organization's DNA,"[41] this also means that data minimization considerations need to be integrated into the entire process. This inherently creates an enormous burden for businesses processing large quantities of data because they will be obligated to determine precisely what user data is necessary from the outset of digital consumer interaction. For businesses that want to analyze sales trends over time, or those that want to provide customers with future recommendations of new products or services, or frankly any company that has a legitimate business purpose for storing data longer than what the GDPR may deem "necessary," this requirement is suffocating. While not impossible, it would prove extremely onerous for businesses to determine what minimum amount of data is adequate to accomplish their goals and properly serve the business interests of their clients.[42]

C. ARTICLE 30: "RECORDS OF PROCESSING ACTIVITIES"

This Article imposes a requirement that companies "maintain a record of processing activities" related to personal data.[43] "Processing activities" is a broad and seemingly all-inclusive term, not explicitly defined within the regulation. Thus, this Article inherently creates an issue of not only how to keep records of processing but also what "processing," if not all, even falls

---

[36] *See id*.

[37] Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1010 (2017).

[38] *Id*. at 1009.

[39] *Id*.

[40] *See id*.

[41] McAllister, *supra* note 34, at 194.

[42] See Zarsky, *supra* note 37, at 1009–11 for a discussion of how the Article 25 restrictions affect "Big Data" companies in particular. While outside the immediate scope of this note, the impact is significant on "big data" companies, and can be helpful in understanding the broader impact of Article 25 across many other industries.

[43] General Data Protection Regulation, *supra* note 1, at 50.

within the scope of this provision.[44] Infringements on the requirements of this Article present the possibility of a ten million euro fine, so it creates a stringent obligation for businesses.[45]

The best solution for achieving compliance with Article 30 would be for businesses to maintain a data processing inventory.[46] Though an inventory format is not explicitly required by Article 30, and could in fact be cumbersome to establish from scratch, an inventory of data can store and present critical information in an effective manner.[47] In fact, the concept of personal data inventories has already been explored and implemented by businesses in several EU countries.[48] Companies already using a data inventory should consider transitioning to a processing data inventory specifically,[49] as it aligns more closely with business functions and renders it easier for businesses to analyze and address privacy concerns.[50] After the core requirements of Article 30 have been met through a processing data inventory, businesses are then free to add further details and information to be stored in the inventory if such storage would help make other data easily accessible.[51] Solutions other than the implementation of a processing data inventory are available to address compliance concerns; however, they are less comprehensive and effective. Rather than standalone, alternative solutions, these options are better treated as supplementary to an efficient processing data inventory. One such supplementary solution is a data flow map, which is a detailed, digital visual representation of the types of data being stored and processed by a business.[52] Though this option may be more cost-effective in a company's immediate future, ultimately it would not be sufficient long-term on its own to serve as a comprehensive, cost-effective solution for businesses.[53]

---

[44] Some international agencies and offices have made an effort to interpret the definition of "processing activities" within the meaning of GDPR Article 30 for the purpose of creating clearer requirements for businesses. One such example is the Information Commissioner's Office of the United Kingdom ("ICO"), which has produced an easy to understand list of processing requirements for both controllers and processors of personal data. *What Do We Need to Document Under Article 30 of the GDPR?*, INT'L COMMISSIONER'S OFF. (ICO), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/what-do-we-need-to-document-under-article-30-of-the-gdpr/.

[45] A PRACTITIONER'S GUIDE, *supra* note 2, at 111.

[46] TERESA TROESTER-FALK & PAUL BREITBARTH, NYMITY INSIGHTS, DOES GDPR ARTICLE 30 REQUIRE A DATA INVENTORY? 1–2 (2017), https://info.nymity.com/hubfs/GDPR%20Resources/Nymity_Insights-GDPR_Article_30_Data_Inventory.pdf.

[47] *Id*. at 2.

[48] *See id*. at 3 (noting that while the concept of data inventories may seem novel, organizations operating in the European Union had already been implementing systems of this nature prior to the GDPR).

[49] *See generally id*. (discussing the distinction between a processing data inventory and a traditional personal data inventory (also referred to as a "data holdings inventory")).

[50] *Id*. at 3.

[51] *Id*. at 4.

[52] Beth Greenall, *How to Comply with Article 30 of the GDPR*, IT GOVERNANCE: IT GOVERNANCE BLOG (June 21, 2018), https://www.itgovernance.co.uk/blog/how-to-comply-with-article-30-of-the-gdpr.

[53] *See id*. (noting that a significant risk of using a data flow map is the inability to access important documents and data should the digital server fail and that this risk needs to be mitigated).

The overarching theme of the requirements set forth by Article 30 is organization.[54] Organizing data processing activities and maintaining an efficient inventory of such data is in a company's best interest.[55] While compliance with Article 30 may seem challenging, it may be worth the burden on businesses. In fact, compliance with Article 30 is arguably essential to compliance with the core articles and purpose of the GDPR as a whole.[56] For example, companies who take the time to ensure complete compliance with the Article 30 requirements also lend themselves to compliance with Article 6 (requiring the establishment of a lawful basis for processing), Article 7 (with conditions and requirements for obtaining consent), and Article 13 (requiring disclosure of the details of processing activity in a privacy notice).[57] Article 30 is thus another example of the interrelatedness of many of the articles of the GPDR, encouraging compliance with the entire regulation through its individual article requirements.

IV. THE GDPR'S EFFECTS ON GLOBAL BUSINESS LITIGATORS AND LITIGATION

It is useful to understand what repercussions the GDPR is already having on business litigators around the globe and their practices, despite the GDPR's relatively recent implementation. In the United States specifically, it has appeared predominantly in the discovery stages of litigation.

Prior to and since the GDPR's implementation in May 2018, litigators have been encouraged to review and familiarize themselves with the GDPR guidelines and to adjust their litigation discovery practices accordingly. For example, rather than solely relying on U.S. discovery rules and practices, litigators may need to consider the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (1970)[58] in light of requirements set forth in Article 48 of the GDPR (governing transfers or disclosures not authorized by EU law).[59] Historically, U.S. judges are impatient with regard to any excessive delays, costs, et cetera associated with complying with a foreign data protection policy, and are skeptical of significant penalties imposed on litigants in other jurisdictions for noncompliance.[60] However, the severity of potential fines under the GDPR suggests a shift in favor of data protection rather than prioritizing typical litigation discovery practices, and cautions litigators and courts to acutely

---

[54] *See The Importance of Article 30 of the General Data Protection Regulation of the European Union (GDPR)*, VERASAFE: THE VERASAFE DATA PROTECTION BLOG (Mar. 9, 2018), https://www.verasafe.com/blog/the-importance-of-article-30-of-the-general-data-protection-regulation-of-the-european-union-gdpr/ (asserting that it is in the best interests of businesses who need to comply with the GDPR to maintain inventories and records of information they process).

[55] *Id*.

[56] *Id*.

[57] *Id*.

[58] ALLEN & OVERY LLP, GDPR FOR LITIGATORS 5 (2018), http://www.allenovery.com/publications/en-gb/Documents/gdpr-for-litigators.pdf.

[59] An in-depth analysis or discussion of GDPR Article 48 is not useful here, nor within the scope of this note. However, see General Data Protection Regulation, *supra* note 1, at 64 for the plain text of the article. *See generally* David J. Kessler, Jamie Nowak & Sumera Khan, *The Potential Impact of Article 48 of the General Data Protection Regulation on Cross Border Discovery from the United States*, 17 SEDONA CONF. J. 575 (2016) (discussing the interpretation and application of Article 48).

[60] ALLEN & OVERY LLP, *supra* note 58, at 5.

weigh and consider the risks of slowing down discovery processes and trials in order to comply with the GDPR (rather than facing massive fines induced by noncompliance).[61] Consequently, for over one year, business litigators have been urged to prepare for the GDPR by gaining a thorough understanding of their corporation's data and processing activities.[62] In preparation for and throughout litigation, litigators have also been advised to consider the rights of data subjects and make reasonable attempts to minimize the involvement of GDPR-governed data in the litigation process.[63]

In theory, based on the above, businesses in litigation with one another could hit a roadblock during discovery if one business is requesting information that falls within the scope of the GDPR. However, in *Finjan, Inc. v. Zscaler, Inc.* (N.D. Cal. Feb. 14, 2019), the court ordered one party to produce certain emails despite the fact that the GDPR may have warranted their protection.[64] Although the defendant contended the emails could not be compelled because of the restrictions within the GDPR, the court noted that another country's statute precluding disclosure of certain evidence would not deprive American courts of the power to compel a party within its jurisdiction to produce evidence, even if doing so would per se violate the statute.[65] The court further explained that several factors surrounding the circumstances of the evidence needed to be assessed in order to determine whether or not to compel evidence, and that if those factors led to the conclusion that the evidence ought to be compelled then the court would rule accordingly.[66] In a similar case, the district court in Utah was unpersuaded by one party's argument that the GDPR necessitated a protective order for certain evidence.[67] The party, a business, argued that opposing counsel's request to compel the data raised tensions with its obligations under the GDPR and the additional steps required to anonymize the requested data were too burdensome.[68] Nonetheless, the court denied the motion for a protective order for the data in question, compelled more by the arguments in favor of producing the evidence than those in favor of protecting it.[69]

These cases demonstrate the U.S. court system's attitude toward the GDPR, which appears to be dismissive at best. It seems that, along with U.S. businesses, U.S. courts do not wish to be bound by the requirements of the GDPR. In *Finjan*, the court explicitly noted that it was not clear enough

---

[61] *Id.*

[62] Bennett B. Borden, Jay Brudz, Jason R. Baron & Yodi S. Hailemariam, *GDPR & Electronic Discovery: What to Do Before, During and After Litigation*, NAT'L L. REV. (Sept. 20, 2018), https://www.natlawreview.com/article/gdpr-electronic-discovery-what-to-do-during-and-after-litigation.

[63] *Id.*

[64] Finjan, Inc. v. Zscaler, Inc., No. 17-cv-06946-JST (KAW), 2019 U.S. Dist. LEXIS 24570, at *10–11 (N.D. Cal. Feb. 14, 2019).

[65] *Id.* at *3–4 (quoting Societe Nationale Industrielle Aerospatiale v. United States Dist. Court for Southern Dist., 482 U.S. 522, 544 n.29 (1987)).

[66] *Id.* at *4 (quoting Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1475 (9th Cir. 1992)). In this case, the court considered the following factors: the importance of the evidence, the degree of specificity of the request for the evidence, whether the evidence originated in the United States, whether the evidence is procurable by alternative means, the extent to which noncompliance would jeopardize the integrity of the United States and its courts, and whether the hardship of producing the evidence outweighs the production of the evidence. *Id.*

[67] Corel Software, LLC v. Microsoft Corp., No. 2:15-cv-00528-JNP-PMW, 2018 U.S. Dist. LEXIS 172875, at *5 (D. Utah Oct. 5, 2018).

[68] *Id.* at *3.

[69] *Id.* at *7–8.

whether one party would be barred from producing the emails in question under the GDPR, particularly because there is no evidence of the extent to which the European governmental bodies are enforcing this regulation.[70] The court emphasized the notion that the company could not produce any evidence as to the likelihood of GDPR enforcement.[71] This attitude toward the GDPR suggests U.S. courts are willing to use American business and judicial interests as excuses to disregard the requirements and implications of the GDPR until there is demonstrative evidence of GDPR enforcement within the United States.[72] This could mean one of two things: either U.S. court officials anticipate that broad comprehensiveness and applicability of the GDPR prohibit strict and consistent enforcement, or they doubt the legitimacy of the GDPR altogether. Despite the fact that litigators have been encouraged to familiarize themselves with the GDPR and the specific data it aims to protect and bar from discovery, courts are dismissive of any such notion and may not feel they have any incentive to honor the guidelines of the GDPR.

V. THE FUTURE OF U.S. DATA PRIVACY LAW AND POLICY AS INFLUENCED BY THE GDPR AND EUROPE

A. THE GDPR AS A POSSIBLE EMERGING GLOBAL STANDARD

To date, the GDPR is the most comprehensive regulation in the realm of privacy law[73] and, in practice, it is broadest in territorial scope.[74] Consequently, it is inevitable that the "application of [the GDPR] will have a huge impact on international data flow."[75] Because so many businesses based outside of the European Union (a notably large amount within the United States) will need to meet the heightened GDPR standard of data processing, arguably the GDPR has set the stage for a new global standard in international data privacy.[76] If the GDPR is setting a global standard, the United States risks falling behind by not passing similar data privacy legislation.[77] Furthermore, the fines imposed on businesses who fail to

[70] *Finjan*, 2019 U.S. Dist. LEXIS 24570, at *10–11.

[71] *Id*. (analogizing to *In re* Air Crash at Taipei, Taiwan on Oct. 31, 2000, 211 F.R.D. 374, 380 (C.D. Cal. 2002), where the court deemed the party had not produced evidence regarding "the manner and extent to which Singapore enforces its secrecy laws").

[72] Finjan was decided in February 2019, at which time there was little evidence enforcement of GDPR fines would occur. Six months later, in August 2019, an article was published online noting that Pricewaterhousecoopers ("PwC") was fined 150,000 euros for violating a GDPR provision. Kate Sukhanova, *PwC Will Have to Work to Rebuild Trust After Shock GDPR Fine*, RECLAIM THE NET (Aug. 11, 2019), https://reclaimthenet.org/pwc-gdpr-fine/. Had this fine been imposed before the decision in Finjan was rendered, it may have persuaded the court to consider the GDPR more seriously. In light of this fine, and any others that may be imposed on other companies for GDPR violations, courts may need to consider the GDPR more strongly.

[73] *See* Samantha Cutler, *The Face-Off Between Data Privacy and Discovery: Why U.S. Courts Should Respect EU Data Privacy Law When Considering the Production of Protected Information*, 59 B.C. L. REV. 1513, 1520 (2018).

[74] *See id.; see also* Allison Callahan-Slaughter, *Lipstick on a Pig: The Future of Transnational Data Flow Between the EU and the United States*, 25 TUL. J. INT'L & COMP. L. 239, 251–52 (2016).

[75] Cutler, *supra* note 73, at 1520.

[76] Callahan-Slaughter, *supra* note 74, at 251–52.

[77] McAllister, *supra* note 34, at 203.

comply with the requirements of the GDPR are so severe in nature[78] that it may be more sensical for the United States, and other regions of the world, to simply adopt the GDPR standard as its own.

In theory, this approach makes sense: The United States adopting a GDPR-like standard would ensure that U.S. companies are both consistently meeting the requirements of their overseas counterparts and, equally important, avoiding devastating monetary sanctions.[79] In reality, it is difficult to imagine what incentive U.S. lawmakers have to conduct such a massive overhaul to current U.S. privacy laws. Although "healthy talks about U.S. efforts to make ongoing improvements to the [data privacy] framework" between U.S. and EU officials have been ongoing, it is unclear how U.S. lawmakers are truly responding to the GDPR.[80] Despite the fact that the issue of data privacy has historically been high on the list of priorities for the U.S. government to address, present-day not excluded, there seems to be little movement toward more comprehensive data privacy protection laws.[81]

The most movement has come in the last year, notably in the latter half of 2018 when the Senate Committee on Commerce, Science, and Transportation (the "Committee") held hearings to discuss potential legislation addressing privacy concerns.[82] The first hearing began with a

---

[78] Fines for GDPR violations can be as hefty as twenty million euros, or four percent of the company's annual global turnover, whichever amount is greater. *E.g.*, McAllister, *supra* note 34, at 196. *See generally Fines and Penalties*, GDPREU.org, https://www.gdpreu.org/compliance/fines-and-penalties/ (last visited Dec. 7, 2018) (outlining the factors considered in evaluating a violation and determining accompanying fines, and explaining the lower and upper limits of fine amounts).

[79] Safari, *supra* note 27, at 848 (asserting that " . . .if companies must adhere to heightened requirements so that they could conduct business in the [European] Union, they might as well implement those safeguards for their employees and American customers, too.").

[80] McAllister, *supra* note 34, at 203 (quoting Angelique Carson, *Safe Harbor-Compliant Companies Seeking Contracts: Facing an Uphill Battle in the EU*, THE INT'L ASS'N OF PRIVACY PROF.: THE PRIVACY ADVISOR (May 20, 2014), https://iapp.org/news/a/safe-harbor-compliant-companies-seeking-contracts-facing-an-uphill-battle-i/).

[81] On average, in 2016, there was one data breach per day (450 total for the year) in the healthcare industry. Dawn Bailey, *One Data Breach Each Day in 2016—Another Reason Experts Say Focus on Cyber Risk Now*, NAT'L INST. OF STANDARDS & TECH.: THE OFFICIAL BALDRIGE BLOG (Jan. 26, 2017), https://www.nist.gov/blogs/blogrige/one-data-breach-each-day-2016-another-reason-experts-say-focus-cyber-risk-now. Of course, 2016 saw data breaches outside the healthcare realm as well. *Id*. At that time, there was a call for stricter data privacy regulations and breach notification policies. *Id*. (statement of Michael Dowling, CEO of Northwell Health) ("Hacking and data breaches are realistic and stubborn dangers we face each day. No [leader] has the luxury of dismissing these threats or viewing the work to prevent them as optional."). While the lack of comprehensive data privacy legislation in the United States seemed to be a grave issue in 2016, it continued to be an issue in 2017 and 2018 with practically no change at the federal level. Late-2018 witnessed another call for progress in privacy, from various senators and groups. Ernie Smith, *Momentum Picks Up for Federal Data Privacy Protection*, ASSOCIATIONS NOW (Nov. 13, 2018), https://associationsnow.com/2018/11/momentum-picks-up-for-federal-data-privacy-protection/. Not six weeks later, however, a hack on Marriott customer data took place, deemed "potentially one of the largest breaches of consumer data in history." Aaron Gregg, *The Cybersecurity 202: Senators Call for Data Breach Penalties, Tougher Privacy Laws After Marriott Hack*, WASH. POST: POWERPOST (Dec. 3, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/12/03/the-cybersecurity-202-senators-call-for-data-breach-penalties-tougher-privacy-laws-after-marriott-hack/5c0436431b326b60d12800d2/?utm_term=.39e5ad1735a1. This hack was followed by yet another outcry for comprehensive data privacy reform at the federal level, yet there has still been no movement. *Id*. While data privacy has seemingly been of the utmost priority to federal legislators for several years, lack of substantive legal reform demonstrates that even in the wake of major data breaches, it may take a long time for the United States to implement data privacy changes of its own.

[82] *E.g.*, Inside Privacy Blog at Covington & Burling, *Senate Discusses a Federal Privacy Law with Privacy Experts: Examining Lessons from the European Union's General Data Protection Regulation and the California Consumer Privacy Act*, NAT'L L. REV. (Oct. 17, 2018),

statement by Committee Chairman John Thune, noting that the hearing was merely the beginning of the Senate's approach toward consumer privacy and "grows out of recent concerns about consumer privacy."[83] The hearings saw disagreement among Committee members about the structure of any potential new federal privacy law.[84] While many agreed that any federal privacy law should preempt current state laws, there was disagreement as to whether such a law would serve as a floor or a ceiling for privacy standards.[85]

For example, states like California have already passed privacy legislation constructed using the GDPR as a model.[86] If potential federal legislation were a floor, any existing state laws requiring a standard higher than the federal law would still be good law, insofar as the requirements not beyond the scope of the federal law do not conflict with the federal requirements. If potential federal legislation were a ceiling, it would override state laws currently in place that hold privacy to a higher standard. Thus, certain data that may be protected under current California law or another state's law could subsequently be unprotected with the enactment of a federal law.

Committee members also voiced concerns about the general heightened standard of the GDPR being too "onerous," asserting that implementing a U.S. law that adopts the GDPR framework would not be feasible.[87] Even if legislators agreed that the GDPR standards were not reasonable and subsequently decided to use state laws—such as the California Consumer Privacy Act ("CCPA")—as the federal framework, they also emphasized the difficulty of creating a GDPR-inspired federal regulation because of conflicting values.[88] One example of conflict is evident in data retention. The GDPR, the CCPA, and other laws generally require data to be stored only as long as it is needed. By contrast, U.S. companies currently have strong financial incentives to keep data for as long as possible.[89] This creates greater potential for data exposure through hacks and breaches of security.[90] It follows that any federal legislation would need to reconcile the financial motivations of businesses to maintain lower standards of data protection and storage with the security policy arguments for maintaining higher standards of data protection and storage.

Should legislators agree to use state laws as a framework, rather than the GDPR, there is still a discussion to be had regarding how to modify the law. The CCPA, and laws similar to it, is designed to regulate data in one state, accounting for a fraction of the data stored and used across the country and

https://www.natlawreview.com/article/senate-discusses-federal-privacy-law-privacy-experts-examining-lessons-european [hereinafter Inside Privacy Blog at C&B].

[83] *Senate Examines Potential for Federal Data Privacy Legislation*, COVINGTON & BURLING: INSIDE PRIVACY BLOG (Oct. 1, 2018), https://www.insideprivacy.com/uncategorized/senate-examines-potential-for-federal-data-privacy-legislation/. "The hearing 'represents the beginning of an effort to inform [the Senate's] development of a federal privacy law.'" *Id*. (quoting Senator John Thune (R-SD)).

[84] *Id*.

[85] Inside Privacy Blog at C&B, *supra* note 82.

[86] California Consumer Privacy Act of 2018, *infra* note 92.

[87] *See Senate Examines Potential for Federal Data Privacy Legislation*, *supra* note 83 ("Several technology company witnesses voiced concerns with adopting a framework similar to the GDPR, which they viewed as onerous.").

[88] See *infra* Part V(E) for further discussion.

[89] Inside Privacy Blog at C&B, *supra* note 82.

[90] *Id*.

around the globe. Committee members have urged that a federal law would need to reconsider certain provisions of state laws, notably their broad scope.[91] Consequently, this forces legislators to return to the aforementioned floor-or-ceiling debate.

Overall, change comes slowly and sporadically,[92] usually as needed and lacking comprehensiveness.[93] Designing and enacting a regulation that mirrors the GDPR standard could prove both expensive and time-consuming; any potential legislation also faces the burden of appealing to the majority of legislators across the political spectrum, which would likely be difficult to accomplish.[94]

B. THE IMPACT OF POTENTIAL LEGISLATION ON SMALL BUSINESSES GENERALLY AND EXCLUSIVELY DOMESTIC U.S. BUSINESSES

Even if one could make the argument that the GDPR should be a global standard to be mirrored in American legislation, there would be significant ramifications of a GDPR-like standard in the United States—particularly for small businesses. Already, small U.S.-based companies who fall under the extraterritorial jurisdiction of the GDPR are struggling to achieve compliance.[95] This is in spite of the fact that some GDPR requirements are waived for smaller businesses.[96] As the aforementioned analysis of the new GDPR requirements illustrates, many U.S. businesses will be conducting "a complete revamping of their software" to meet compliance standards.[97] This process will require a substantial set of resources that small businesses simply cannot spare.[98] Consequently, small U.S. businesses are caught "between a rock and a hard place"[99]: either they pour vital resources into a complete reconfiguration of their data processing technology, likely threatening the revenue from whatever product or service they offer, or they

---

[91] *See Senate Examines Potential for Federal Data Privacy Legislation*, *supra* note 83 (" . . .several provisions of [the CCPA], such as the non-discrimination provision and the broad definition of personal information, should be reconsidered before using it as a model for potential federal legislation.").

[92] Gregg, *supra* note 81. It is also important to note that the lack of consistency among state privacy laws adds to the sporadic and inconsistent change seen in the United States. For example, the most recent significant privacy law comes from California by means of the California Consumer Privacy Act of 2018. CAL. CIV. CODE tit. 1.81.5 (Deering 2018) (operative 2020) [hereinafter CCPA]. It was passed in 2018 but will not be operative until January 1, 2020. *Id*.

[93] *See* Gregg, *supra* note 81. The most recent federal legislation addressing data privacy was several years ago and was far from comprehensive. *Id*. ("The last major U.S. corporate cybersecurity overhaul was the 2014 Cybersecurity Enhancement Act, which led to a voluntary set of standards managed by the National Institute for Standards and Technology (NIST). That law doesn't include fines for violations or data breaches.").

[94] *See, e.g.*, *id*. ("It is unclear, however, how [data privacy] legislation would fare in a split Congress that appears poised for gridlock.").

[95] *See* McAllister, *supra* note 34, at 200–01 (explaining the hardship facing small businesses who are subject to the GDPR).

[96] For example, businesses "with fewer than 250 employees are not required to keep records of their processing activities unless processing of personal data is a regular activity." *EU Data Protection Reform: Better Rules for European Businesses*, EUR. COMMISSION, https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-business_en.pdf (last visited Nov. 7, 2018). Because even exemptions of requirements have restrictions and exceptions, it is in the best interest of small businesses to treat themselves as necessarily within the scope of the GDPR.

[97] McAllister, *supra* note 34, at 200.

[98] *Id*. at 200–01.

[99] *Cf*. *id*. at 200 (arguing that small businesses are "caught 'between a rock and a hard place'" because they must either force themselves to comply with the GDPR or stop servicing EU customers).

are sanctioned with a GDPR violation fine that is so severe it nearly bankrupts them.[100] A third option is for those companies to stop servicing European consumers—however this would also be financially detrimental.[101] As a result, complying with the new data protection regulation proves to be too great of a burden for U.S. small businesses to bear.[102]

This problem would increase tenfold if the United States adopted domestic data privacy legislation mirroring the GDPR. The number of U.S.-based companies falling within the GDPR's jurisdictional reach is large, but it does not encompass all U.S. businesses. Thus, comprehensive, GDPR-like privacy legislation in the United States would force businesses who would not ordinarily be subject to the heightened requirements of the GDPR to conduct the same revamping of internal data processing as their GDPR-compliant peers. Suddenly, companies who never thought twice about the GDPR and its newly implemented requirements would be pouring resources into achieving compliance with a similar federal law, potentially at the expense of conducting business. In fact, some legislators have argued that implementing legislation that mirrors the requirements of the GDPR "could harm 'innovative and entrepreneurial businesses.'"[103] This would inevitably prove especially daunting for small businesses, as they suffer the most in the race to compliance. Additionally, however, new businesses may be adversely affected. Some legislators assert that a newly-implemented privacy law would favor incumbent players over new entrants in any given industry.[104] Of course, any business new to a marketplace or exposed to privacy requirements for the first time will have trouble "catching up" to seasoned players who may have had some privacy measures in place already. If the United States can barely monitor the businesses who are currently subject to the GDPR and guide them toward compliance,[105] what incentive does it have to further subject any remaining domestic businesses to the same heightened standards?

C. WHAT MIGHT FUTURE U.S. LEGISLATION LOOK LIKE?

Amid these concerns, there has, however, been proposed legislation in the wake of the GDPR in an effort to address data privacy concerns. One such example is the Customer Online Notification for Stopping Edge-provider Network Transgressions (commonly referred to as the "CONSENT Act"), introduced in April 2018 by Senator Ed Markey (D-MA).[106] The

---

[100] *See id*. at 201.

[101] *See id*. at 200 n.134 (citing Angelique Carson, *Safe Harbor-Compliant Companies Seeking Contracts: Facing an Uphill Battle in the EU*, THE INT'L ASS'N OF PRIVACY PROFESSIONALS: THE PRIVACY ADVISOR (May 20, 2014), https://iapp.org/news/a/safe-harbor-compliant-companies-seeking-contracts-facing-an-uphill-battle-i/ (" . . .U.S. companies seeking to transfer data out of the EU [are] 'stuck between a rock and a hard place'").

[102] *Id*. at 201.

[103] *Senate Examines Potential for Federal Data Privacy Legislation*, *supra* note 83.

[104] *Id*.

[105] *Cf*. Kris Lahiri, *U.S. Businesses Can't Hide from GDPR*, FORBES: FORBES TECH. COUNCIL (Mar. 27, 2018, 7:30 AM), https://www.forbes.com/sites/forbestechcouncil/2018/03/27/u-s-businesses-cant-hide-from-gdpr/#2efb00cb52c8 (asserting that seventy-nine percent of U.S. businesses [subject to the GDPR requirements] had no plan in place to address compliance or perhaps did not fully understand the weight of the requirements).

[106] Customer Online Notification for Stopping Edge-provider Network Transgressions Act, S. 2639 115th Cong. (2018) [hereinafter CONSENT Act].

CONSENT Act unofficially died with the congressional turnover in January 2019, but is worth analyzing as a good example of proposed privacy legislation that could be reintroduced in the current or a future Congress.

1. The CONSENT Act as a First Step

This proposed bill is nowhere near as comprehensive as the GDPR, but serves as a plausible example of what the first step in data privacy legislation might look like in future U.S. legislation. The CONSENT Act is designed to apply to providers of "edge services," which, broadly defined, includes most Internet-based services.[107]

Compared to the GDPR, the CONSENT Act is small in scope and weak in reach. The Act specifically addresses the handling, use, and storage of customer personal data[108] but has nowhere near the strictly outlined requirements of the GDPR. The Act would require edge providers "to notify a customer about the collection, use, and sharing of the sensitive customer proprietary information of the customer."[109] Specifically, customers must be notified as to the type of information being collected and the purposes for which the information is being used.[110] The notification must take place both when a customer initially forms a relationship with the edge service provider as well as if or when the data-related policies of the provider change in a significant way.[111]

Noticeably absent from this proposed legislation is any right for consumers to request access to the data stored by providers or to receive a simplified report in a readable format of the data being stored or used by the provider. This may be a result of a fundamental difference in purpose behind this potential legislation and the GDPR (and other legislation mirroring the GDPR). While setting restrictions and requirements for businesses is evident in the plain text of the GDPR, the regulation's purpose is first and foremost the emphasis on and protection of a personal right to data privacy.[112] The GDPR is inherently more consumer-friendly and detailed as to the rights held by consumers because of the European emphasis on privacy as a fundamental right.[113]

By contrast, the proposed CONSENT Act focuses on the responsibilities of service providers, not on the rights of consumers. In fact, the CONSENT Act requirements offer no specifications as to what processes providers must implement. The language used within the proposed legislation includes

---

[107] *Id*. The CONSENT Act applies to "edge providers," defined by § 2(a)(4) as "a person that provides an edge service, but only to the extent to which the person provides that service." *Id*. The Act establishes criteria for what constitutes an "edge service," but the term generally encompasses most Internet-based services. *See id*. § 2(a)(5) (defining the term "edge service" using broad criteria).

[108] *See id*. § 2(b)(2)(B)(i) (discussing the requirements under the regulation dealing with "sensitive customer proprietary information of the customer").

[109] *Id*.

[110] *Id*.

[111] *Id*. § 2(b)(2)(B)(ii).

[112] *See* General Data Protection Regulation, *supra* note 1, at 1 ("The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.").

[113] This concept is discussed at length *infra* Parts V(D) and V(E).

requiring edge providers to "implement strong protection for sensitive customer proprietary information"[114] and "develop reasonable data security practices."[115] Standards of "strong" or "reasonable" are vague and opaque and leave enormous freedom for businesses to exercise discretion as to what constitutes "strong protection" or "reasonable practices."

In response to such broad and ambiguous language, one might predict that the enforcement component of the bill is stringent and well-defined. The GDPR, for example, outlines severe repercussions companies could face should they fail to comply with the requirements outlined in the regulation, notably fines of up to tens of millions of euros.[116] However, the CONSENT Act provides for no such measures; the Act instead defers to the Federal Trade Commission ("FTC") Act, stating that "a violation of [the CONSENT Act] or a regulation prescribed under [the] Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under . . . the Federal Trade Commission Act."[117] The language subsequently found in the FTC Act bears no resemblance to that found in the GDPR.[118]

This level of deference is not seen in the GDPR or any other international legislation like it, and is indicative of what kind of legislation the United States would likely pass in coming years (regardless of whether it is the CONSENT Act, a variation of it, or an entirely different piece of legislation). If the CONSENT Act is any indication of the direction that U.S. privacy legislation is headed, it is obvious that the strength, enforceability, and overall impact of such legislation would be minimal at best. This may in fact be intentional.[119] If U.S. legislators are not taking privacy concerns as seriously as their European counterparts, legislation to the effect of the CONSENT Act may simply be an attempt for the United States to cover its proverbial rear, establishing privacy standards in theory but in practice fostering little to no sense of responsibility toward consumers on the part of businesses.

There is also the issue that individual states feel differently about the regulation, protection, and privacy of data. Realistically, any federal legislation would preempt state laws regarding data privacy, so it is critical to recognize that this may inherently create tension between the priorities and goals of federal legislation and those of state legislation. Currently, there are vast differences among states in the level of regulation and protection of

---

[114] CONSENT Act, *supra* note 106, § 2(b)(2)(B)(iv).

[115] *Id*. § 2(b)(2)(B)(vii).

[116] *Fines and Penalties*, *supra* note 78.

[117] *Id*. § 2(c)(2).

[118] *See* 15 U.S.C. § 57a(a)(1)(B) (2018) (including the specific language of the Federal Trade Commission Act that is referenced by the CONSENT Act § 2(c)(2)).

[119] While there is no explicit indication that loosely designed privacy legislation is an intentional act by legislators for the mere sake of appearances, there has been obvious discord between legislators in determining whether harsh regulation of data activity is beneficial for or detrimental to businesses. *See Senate Examines Potential for Federal Data Privacy Legislation*, *supra* note 83.

At the hearing, senators disagreed about the model for any potential new federal privacy law. Senator Jerry Moran (R-KS) pushed back on suggestions that a new federal law should adopt either the approach embodied by the EU General Data Protection Regulation ("GDPR") or the California Consumer Privacy Act ("CCPA"). Rather, he argued that adopting those laws in the United States could harm "innovative and entrepreneurial businesses. *Id*.

There has not been any apparent, strong bipartisan support for what ought to be included in potential privacy legislation beyond "certain broad privacy principles that could be incorporated into legislation." *Id*.

consumer data. Almost every state within the United States has a different definition of "personal information."[120] Some definitions are broader than others,[121] and while certain data are considered "personal information" across all states[122] there is, overall, a lack of consistency across states. Standardizing definitions of terms such as "personal data," "security breach," and "required notification" through the enactment of federal data privacy legislation would be a good first step to establish consistency.

However, this is not without its challenges. First, legislators are forced to return to the floor-or-ceiling debate because states have such broad discrepancies. Second, some states have re-worked their definitions of these types of terms in light of the implementation of the GDPR, in order to ensure there would be no issues of compliance.[123] Whatever federal legislation is subsequently enacted, the definitions provided therein would need to be reflective, to at least some degree, of the GDPR standard in order to honor those efforts by state legislatures to do so. If not, the federal government could face backlash from states, especially those who have implemented very comprehensive legislation complying with the GDPR standard.[124]

2. Tackling Data Breaches

In addition to focusing on data privacy generally, federal privacy legislation would likely be expected to address data breaches specifically, including protection and notification for consumers. The United States, in particular, has been experiencing severe data breaches for the last decade, with the number of breaches significantly increasing as an influx of online activity results in increased personal data transactions across Internet platforms.

---

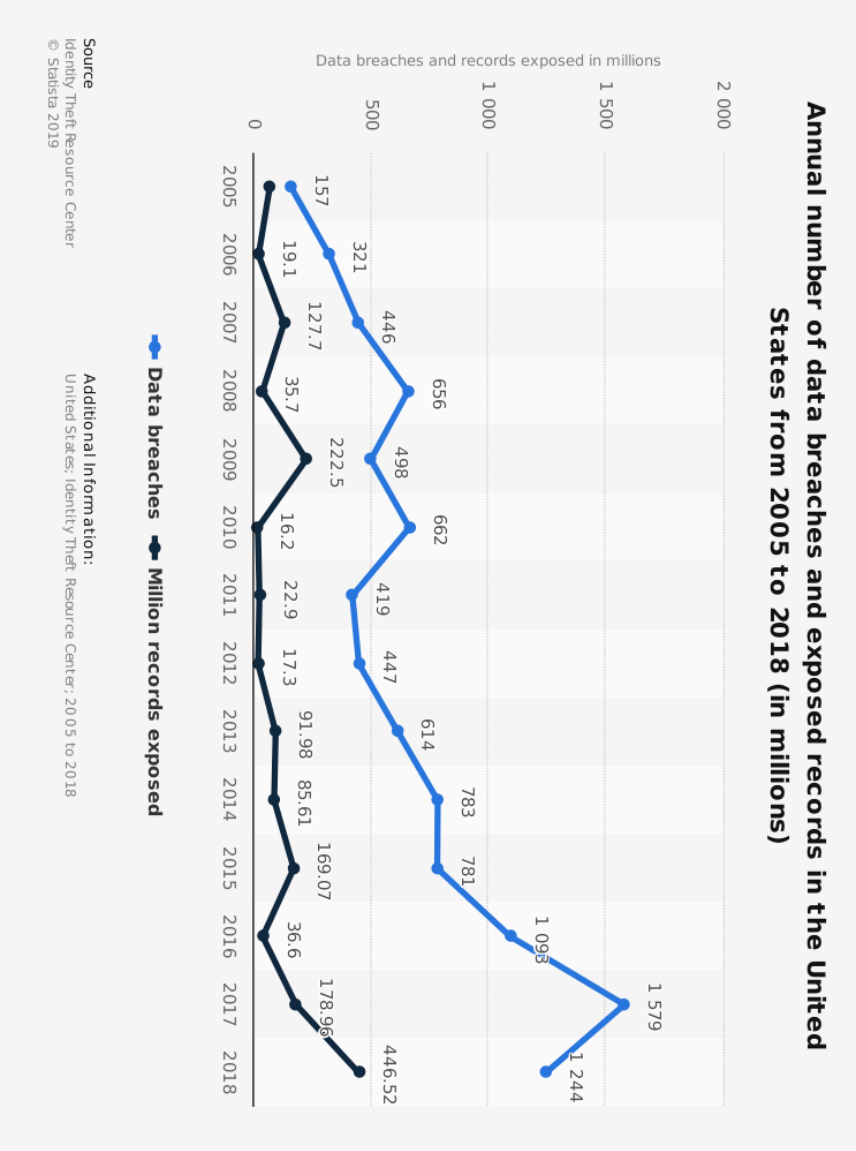
[120] *See* BAKERHOSTETLER, DATA BREACH CHARTS 2–9 (2018), https://www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf (listing every U.S. state whose definition of "personal information" as it relates to privacy legislation is different from the standard definition on page 1).

[121] *Id*.

[122] *See, e.g.*, *id*. at 1 (an individual's first name or initial and last name are considered personal information by default, followed by other examples).

[123] *See id*. (published in July 2018 and including the most updated state legislation information after the GDPR went into effect in May 2018). Between the passage of the GDPR and its enactment, some states adjusted their privacy laws and definitions in order to be GDPR compliant.

[124] A notable example of one of these states is California, which has worked hard to design and implement the CCPA and whose legislators may be frustrated with the federal government if it does not show a similar level of effort or initiative.



The above chart is a graphic representation of all data breaches in the United States from 2005 to 2018 as well as the number of personal records exposed through those breaches.[125] There are two noteworthy conclusions to draw from this chart. First, data breaches in general have been a growing problem over the last decade. Over the course of five years, from 2013 to

[125] Identity Theft Res. Ctr., *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2018 (in millions)*, STATISTA, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last visited Mar. 2, 2019).

2018, the total number of breaches in the United States more than doubled.[126] Data breaches are garnering more attention as they become more frequent, due in part to the increased use of digital files and consumer reliance on digital data and platforms.[127]

Second, and perhaps more importantly, data breaches are becoming more severe. For example, while the number of total breaches noticeably decreased from 2017 to 2018, the number of exposed personal records more than doubled between 2017 and 2018.[128] This means that even if the number of breaches is decreasing, the volume of compromised information is increasing, resulting in more detrimental breaches than in years past. One of the biggest leaps in exposed records in recent history was in 2017,[129] likely a result of both the sharp increase of total breaches and the sources of those breaches. For example, a major data breach of the credit reporting agency Equifax in 2017 accounted for the exposure of potentially over one hundred million individual records of personal information. In 2018, another major breach, this time of the Marriott data stores, resulted in one of the highest numbers of exposed consumer personal data records in recent history.[130]

While data breaches affect a myriad of industries every year, the business sector has had the greatest stake in the matter. In fact, the business sector accounted for over 90 percent of all exposed records in 2017, resulting in losses of tens of millions of dollars to businesses and financial service providers over the past several years.[131] Thus, businesses would presumably have the most to gain from federal data privacy legislation that addressed security breaches.

In theory, this is true. In practice, this is most likely false. One of the major areas potential breach-related legislation would address is "notification." Notification refers to the policies and procedures businesses must have in place to notify consumers of any potential or realized data breach and exposure of personal information. The GDPR handles notification throughout the regulation, stressing open and prompt communication with consumers regarding storage and potential breach.[132]

By contrast, although all fifty states have enacted legislation requiring businesses to notify consumers of personal data security breaches,[133] notification laws and policies remain inconsistent in the United States. Similar to the inconsistencies in general privacy legislation and definitions of specific data-related terms, there is ample inconsistency among state data breach notification laws. Many states, such as Alabama, Iowa, and Oregon,

---

[126] *Id*.

[127] *Id*. While this chart displays data only from the United States, data breaches are creating concern across the globe. In fact, identity theft through digital data breach accounted for fifty-nine percent of breaches worldwide in 2016. *Id*. The prevalence of digital data breaches was almost certainly a major factor in the drafting and enactment of the GDPR.

[128] *Id*.

[129] *Id*.

[130] Gregg, *supra* note 81.

[131] Identity Theft Res. Ctr., *supra* note 125.

[132] *See generally* General Data Protection Regulation, *supra* note 1.

[133] *Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx#1 (last updated Sept. 29, 2018).

endured a process of trial and error, with state legislatures proposing several bills until one was finally enacted.[134]

Because the general nature of data breach notification laws tends to be reactive, meaning legislation is often enacted in response to problems rather than as a preemptive measure, many state breach notification laws reflect state-specific issues addressed by the legislation. This also helps account for the inconsistency across state laws. For example, breach notification laws in Nebraska revise provisions of the Credit Report Protection Act and the Financial Data Protection and Consumer Notification of Data Security Breach Act, reflecting concern for personal information stored with credit reporting agencies, likely in light of the Equifax breach in 2017.[135] Breach notification laws in New Mexico mirror these Equifax-related concerns as well.[136]

By contrast, other states may still be incorporating Equifax-related provisions into their breach notification laws but are prioritizing other provisions. For example, breach notification laws in Ohio actually provide a legal safe harbor to covered entities that implement a specified cybersecurity program.[137] This approach is designed to reward and protect businesses who take the necessary measures to prevent breaches from happening in the first place, rather than simply listing consumer rights and business obligations once a breach has already occurred.

Other states, such as Alabama, Arizona, and Colorado, have enacted breach laws that generally "cover the basics" related to personal information and data breaches, without specific industry-related provisions (such as Equifax-inspired concerns).[138] The legislation in these states can lack the targeted reach of states like Nebraska and New Mexico, and/or the positive reinforcement incentives found in Ohio's legislation.

The discrepancies in state breach notification laws are emblematic of a difference in priorities and goals across the United States. This again raises the question of preemption. If proposed federal privacy legislation intends to preempt state laws in the area of breach notification as well, the task of creating a comprehensive piece of legislation has now become infinitely more difficult. The need for broad legislation that considers aforementioned states' goals to explicitly include policies for credit reporting agencies or to incentivize businesses to prioritize protecting consumer data and communicate breaches to consumers will be in direct conflict with businesses' goals of avoiding strict federal regulation and the embarrassment that accompanies notifying customers of a suspected or actual data breach.

Although the goal of potential federal privacy legislation may be to address both the privacy and the protection of personal data on a general scale, and the policies and procedures related specifically to data breaches

---

[134] *2018 Security Breach Legislation*, NAT'L CONF. OF ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/2018-security-breach-legislation.aspx (last updated Feb. 8, 2019).

[135] *Id*.

[136] *Id*.

[137] *Id*.

[138] *See id*.

and notification, this may be too ambitious.[139] It would perhaps be more prudent for the federal government to pass a series of privacy laws, each one addressing certain data concerns, instead of designing and implementing one enormous, all-encompassing piece of legislation. In support of this approach, businesses would have a greater opportunity to adapt their practices and policies to ensure compliance with forthcoming U.S. law. This approach also allows legislators to carefully and meticulously craft legislation that would reflect the efforts states have made thus far to protect consumers. However, a significant concern with this approach would be time: it would almost certainly take years to implement staggered regulations considering that the CONSENT Act was introduced in April 2018 and was not enacted before the turn of Congress in January 2019 (despite co-sponsorship by several senators). By the time a series of laws were enacted, some may be outdated in light of newly arising privacy concerns or newly-targeted industries. Thus, it seems that the federal government has no clear path to all-inclusive data privacy legislative reform.

D. CREATING (OR EXACERBATING EXISTING) TENSIONS BETWEEN THE UNITED STATES AND EUROPE

With the implementation of the GDPR, the European Union has arguably positioned itself as "a leader in the realm of data protection law in the digital economy."[140] In fact, Europe's regard for data privacy as a fundamental right deserving authoritative government protection separates it from the rest of the world,[141] including the United States, where privacy is not inherently considered a fundamental human right.[142] Accordingly, the European Union embraces a much greater expectation of privacy than what has existed historically or currently exists in the United States.[143]

In fact, this stark difference in the treatment of data privacy between Europe and the United States was a major factor pushing the development of the GDPR in Europe.[144] Europe felt that U.S. laws inadequately served European citizens and their right to data privacy[145] and sought to replace the then-existing 1995 Directive[146] in order to compel the United States and others to hold data privacy to the same standard as the European Union.[147]

---

[139] Consider that the GDPR attempts to act as comprehensive data reform, including specific information regarding suspected or actual breach of secured data. The English version of the GDPR is eighty-eight pages in length. General Data Protection Regulation, *supra* note 1. By contrast, the aforementioned CONSENT Act, used to help anticipate what future privacy legislation will look like in the United States, is a humble fifteen pages in length. CONSENT Act, *supra* note 106. Of course, the GDPR was designed and drafted over a much lengthier period of time than the CONSENT Act was; however, even a mere comparison of the number of pages suggests the GDPR was designed to be all-encompassing, long-lasting, and effective while the CONSENT Act seems only to partially address privacy concerns in the United States.

[140] McAllister, *supra* note 34, at 210.

[141] *Id*.

[142] Eaton, *supra* note 4.

[143] McAllister, *supra* note 34, at 189.

[144] *See id*. at 189–90.

[145] *Id*. at 190.

[146] Refers to European Union Directive 95/46/EC, commonly referred to as the "1995 Directive," and is now replaced by the GDPR regulation.

[147] *See* McAllister, *supra* note 34, at 190. The 1995 Directive was not as comprehensive or enforceable, nor did it achieve the data privacy goals of Europe, as compared to the GDPR. *See GDPR*

Was it Europe's goal, in passing the GDPR, to set a global standard? It is a possibility. Perhaps Europe anticipated that the passage of the extraterritorial GDPR would strongly encourage, if not compel, the GDPR to set the global standard, essentially forcing the rest of the world to prioritize and protect consumer data privacy to the same degree as Europe. This suggests the GDPR was a somewhat aggressive measure by the European Union.

The alternative view is that the passage and implementation of the GDPR was more likely a defense mechanism than an act of aggression or dominance. The lack of consistency in the treatment of personal data and privacy among Europe, the United States, and the rest of the world created a level of distrust in Europe, particularly with the United States.[148] A lack of proper privacy laws in the United States in particular, a major processor of consumer personal data, "sowed distrust around the world with respect to the [U.S.] treatment of personal data."[149] A continual and growing lack of confidence may have led the European Union to feel threatened regarding the protection of personal data within its borders; Europe could never afford to stop interacting with foreign markets or subscribing to foreign services, so the GDPR may have been a tactic to protect European citizens' data in a time of deep distrust.

Hence, an incentive for the United States to adopt legislation mirroring the GDPR may be to help mitigate these tensions with Europe in the realm of cybersecurity. An implementation of GDPR-like legislation could be considered by Europe as a sign of good faith, a showing by the United States that it respects the value that Europe has placed on the protection of personal data. Alternatively, even absent a comprehensive overhaul of privacy laws, the United States could still respect the European value that privacy is a fundamental human right by creating minimal requirements that encourage U.S. businesses, and even court systems, to place a similar emphasis on user data privacy.[150] However, considering the aforementioned burden the implementation of such legislation would have on many U.S. businesses,[151] notably financial risk, an "olive branch" to Europe may not be incentive enough.

E. THE BALANCING ACT: MERGING THE U.S. VALUE OF DEREGULATION OF BUSINESS PRACTICES AND THE EU VALUE OF PRIVACY AS A FUNDAMENTAL HUMAN RIGHT

If an "olive branch" alone is insufficient to incentivize U.S. legislators to implement comprehensive data privacy reform, the addition of a value aspect for U.S. citizens may help. A multitude of polls demonstrate that the majority of U.S. citizens are to some degree concerned about data privacy

Key Changes, EUGDPR.ORG, https://eugdpr.org/the-regulation/ (last visited Dec. 8, 2018) (" . . . territorial applicability of the [1995 Directive] was ambiguous and referred to data process 'in context of an establishment.'").

[148] *See* McAllister, *supra* note 34, at 200 n.134, 210.

[149] *Id*. at 210.

[150] *Cf*. Cutler, *supra* note 73, at 1539 (asserting that absent domestic legal reform, U.S. courts maintaining the same [or a similar] standard to Europe could be a showing of respect [and good faith]).

[151] *Supra* Part V(B).

and controlling their personal information.[152] In recent years, citizens and lawmakers alike have called for stronger protection of personal privacy.[153] In light of major data mega-breaches like the Equifax breach in 2017 and the Marriott breach in 2018, the call for reform has only grown louder.[154] But, is it loud enough to implement a U.S. version of the GDPR?[155] It is possible, but any legislation would surely have an American twist.

Inarguably, data privacy is worthy of protection in the United States, but the degree of protection almost certainly would not match the harsh requirements of the GDPR for two primary reasons. First, while U.S. citizens and lawmakers value privacy protections, they also value deregulation and free trade.[156] Data privacy itself is a field that is vastly unregulated, and generally has always been that way.[157] Extensive and specific requirements imposed on business practices, like those outlined in Articles 15 and 30 of the GDPR, would be met with an outcry from staunch supporters of deregulation, including the current U.S. administration.[158] Deregulation has been consistently on the rise in the last two years,[159] so it does not seem likely that a detailed, all-encompassing, micromanaging rulebook like the GDPR is going to be set forth any time soon. Or, at the very least, even if a regulation of such nature were to be introduced in the legislature, it is very possible it would not survive a bipartisan vote.[160]

Second, even if lawmakers across the political spectrum came together and constructed a reformative data privacy and protection policy, the implementation stage would face challenges. Setting restrictions or limitations on the type or quantity of private user information that businesses can store would not be realistic for many U.S. companies.[161] Businesses that handle large and complicated influxes of personal data inherently almost always have a need to collect sensitive data and store it for extended periods

---

[152] Cutler, *supra* note 73, at 1538 (citing Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 355 (2015)).

[153] *Id*.; *see* Gregg, *supra* note 81.

[154] Gregg, *supra* note 81.

[155] An additional consideration is the potential public and political backlash following disclosure that U.S. businesses provide more extensive protection to the personal data of foreign customers than of American citizens. Zarsky, *supra* note 37, at 1018–19. While this concern is not invalid, it has not yet manifested itself. To date, American citizens in possession of the knowledge that only foreign customers get the benefit of heightened security precautions have not proven a concern the U.S. federal administration.

[156] *See* William Dunkelberg, *Why Deregulation Is Important*, FORBES (Mar. 23, 2018, 2:23 PM), https://www.forbes.com/sites/williamdunkelberg/2018/03/23/why-deregulation-is-important/#59a9fa661c18 (arguing that deregulation consistently plays a critical role in economic growth, and that cutting regulations and their accompanying costs is better for continued business and economic development).

[157] *See* Gregg, *supra* note 81.

[158] *See* Terry Jones, *Deregulation Nation: President Trump Cuts Regulations at Record Rate*, INV. BUS. DAILY: COMMENT. (Aug. 14, 2018), https://www.investors.com/politics/commentary/deregulation-nation-president-trump-cuts-regulations-at-record-rate/ (discussing how President Donald Trump, along with his administration, has met and surpassed deregulation goals, and began cutting rules and regulations at a steady pace since entering office in January 2017).

[159] *See id*.

[160] *Supra* note 94.

[161] *See* Gregg, *supra* note 81 ("Ron Gula, a cybersecurity investor who founded Maryland-based cybersecurity company Tenable Network Security, said [legislators'] idea [of] setting limits on personal information that companies can store would not be realistic for companies like Marriott [who suffered a massive security breach in November 2018] . . . . ").

of time.[162] For example, it cannot be expected that companies like Equifax just dispose of personal data on a regular basis. Hence, if a privacy regulation in the United States is designed to be comprehensive and detailed, the language would have to outline specific requirements for businesses in particular industries who handle distinct types of data and who offer specific services. That is a task no legislator is up for.

With deregulation and feasibility concerns in mind, it seems the most plausible U.S. legislation tackling data privacy would need to: (1) establish a minimum standard of data security that is both achievable and widely applicable, and (2) focus heavily on fines and sanctions.[163] Currently, U.S. businesses rarely face fines for private data misuse or breach, so instituting a legitimate penalty system could be the push that businesses need to start prioritizing data privacy.[164] However, the implementation of a new set of data security requirements establishing a penalty system for failure to meet the minimum standard—including fines for institutions and prison terms for individual offenders—could have an adverse effect.[165] Rather than demonstrating a genuine investment in security and integrating data privacy into the mission of their business, companies would more likely simply focus on meeting whatever bare-minimum standard the legislation creates in order to avoid monetary penalties.

Thus, it seems that a policy which preserves the EU value of privacy as a fundamental right would smother the U.S. value of deregulation, and any attempt at incorporating the EU value of privacy into a less stringent regulation has little chance of bringing about true reform. Though grim, the notion that the two cultural values might never coexist in U.S. data privacy legislation is not far-fetched.

VI. CONCLUSION

Today, data privacy is centerstage. The GDPR has come into force, and businesses around the world, including those in the United States, are paying attention. The regulation has claimed jurisdiction over U.S. companies conducting business in Europe, mandating strict compliance with newly implemented requirements with the prospect of severe financial sanctions for noncompliance. The most stringent of new obligations imposed on businesses fall under the category of mechanisms for processing personal data and managing consumer data inquiries. Now, U.S. businesses must have in place a comprehensive, organized, automated system of organizing and storing personal data and responding to a consumer inquiry on the substance

---

[162] *See id*. (statement of Ron Gula) ("When you book a Marriott hotel room it's kind of nice that they already have all of your information when you book a room . . . they are always going to have to collect sensitive data on their customers . . . ."). The nature of businesses like hotels (e.g., Marriott) or credit reporting services (e.g., Equifax) inherently create a need to collect extensive personal data from customers and store the data for almost inevitable future use. *See id*. For example, it is not unreasonable that a hotel like Marriott would be frequented more than once by an individual—the convenience of having your personal information auto-filled and recognized by the hotel booking portal is only possible if the business is permitted long-term storage of personal data. *Id*. Equifax works in a similar fashion—chances are high that if an individual requested their credit score report once before, at some time in the future they will request it again.

[163] *See id*.

[164] *Id*.

[165] *Id*.

and status of stored information—a right which consumers can exercise at any time for any reason. Data privacy, by some mechanism, must be inherent in the way companies conduct business with European clients and the personal data they submit.

Has the GDPR made a global footprint? Undoubtedly. The GDPR took the world by storm and inherently forced every region of the world that services European clients to self-reflect on their own treatment and protection of personal data. The GDPR brought about global recognition of the European standard of data privacy. But it may be premature to say that it has set or is the new standard. The United States may be home to businesses that fall within the jurisdiction of the GDPR, but it has not made any noticeable movement toward implementing its own legislation matching the caliber of its colleague across the pond. With few or no financial incentives to implement a comprehensive privacy policy, the United States is unlikely to follow suit. Furthermore, if the United States has any interest in repairing the eroded, distrustful relationship with Europe regarding the quality of data protection, it has not demonstrated so. On the contrary, the U.S. courts have proven dismissive of the regulation and its requirements, openly doubtful of its severity and enforcement, and unwilling to incorporate it into the basic discovery process of U.S. litigation. Indeed, U.S. history of data privacy and protection leads to the conclusion that no comprehensive data privacy reform will take place until the need arises—either U.S. data breaches will be so severe and so frequent that legislators will have no choice but to act, or the global privacy standard will have evolved so much that inaction would put the United States at a competitive disadvantage. At that time, it will be up to U.S. legislators and leaders to work together and design a transformative solution to the issue of data privacy that both respects and protects user data as well as, at the minimum level, polices companies and the manner in which they conduct business.