THE DATA PRIVACY REVOLUTION: HOW THE ERA OF THE GENERAL DATA PROTECTION REGULATION IMPACTS TENNESSEE BUSINESSES

T. Bruce Shank II*

I. Introduction

On April 14, 2016, the European Union passed the General Data Protection Regulation ("GDPR"), which went into effect on May 25, 2018.[1] The GDPR declares "the protection of natural persons in relation to the processing of personal data" as a fundamental right.[2] The European Union views personal data as belonging to the user, while the United States sees it as belonging to the business that controls it.[3] In the United States, "data privacy law is based on the idea of consumers whose interests merit governmental protection in a marketplace marked by deception and unfairness."[4] The United States, as a result, deals with privacy issues as the need arises. While the European Union emphasizes consent and contract in data processing, the United States' data privacy law lacks these doctrines.[5] The opposing views on data privacy create tension between the GDPR's sweeping reform, and the hands-off approach of the United States.

Data privacy in the United States operates under a patchwork of federal and state laws, and Tennessee will act as an exemplar to examine

* J.D. Candidate 2020, University of Tennessee College of Law; B.A. 2017, University of Tennessee – Knoxville. I would like to thank my wife, Chloe, and my mentors, David Morehous and Haseeb Qureshi.

[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 Council Directive 95/46/EC, 2016 O.J. (L 119) 59 cor. 2018 O.J. (L 127) 61 [hereinafter "GDPR"].

[2] *Id.* recital 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.").

[3] *See* Paul M. Schwartz & Karl-Kiolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 120 (2017).

[4] *Id.* at 119.

[5] *Id.*

the United States approach.[6] Further, Tennessee businesses that conduct business with European Union residents will be subject to the GDPR.[7] The penalty for noncompliance can be substantial.[8] This paper does not mean to provide an exhaustive list of requirements for GDPR compliance, but instead spotlights pressing issues that will likely affect Tennessee businesses, as well as an analytical approach to the GDPR and its impact on the data privacy law in the United States.

Part II begins with a background of the GDPR, its definitions, the Privacy Shield agreement between the United States and European Union, and federal and state laws that impact data privacy in Tennessee. Part III explores the GDPR, including the fundamental principles and rights, compliance standards, relevant case law in Europe and the United States, and the major criticisms of the Regulation. Part IV questions the future of data privacy in Tennessee by first considering the recent developments around the United States and then making a case for adopting a GDPR-like privacy regulation. Lastly, Part V concludes with a summarization on the importance of the GDPR in Tennessee and reiterates the potential for similar laws to develop in the United States.

II. Background

A. Overview of the General Data Protection Regulation

Before the GDPR, the European Data Protection Directive of 1995 ("the Directive") regulated personal data transfers within the European Union.[9] The GDPR repealed and replaced the Directive on May 25, 2018.[10] While the Directive was not directly binding on European Union member states, the GDPR created directly enforceable privacy standards.[11]

The territorial scope of the GDPR applies to the processing of personal data in three situations.[12] First, the GDPR applies to the processing of personal data when a controller or processor is established

---

[6] *Id.* at 135.

[7] GDPR, *supra* note 1, art. 3.

[8] *Id.* arts. 83-84.

[9] Schwartz & Peifer, *supra* note 3, at 128; *see also* Council Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC).

[10] GDPR, *supra* note 1.

[11] Schwartz & Peifer, *supra* note 3, at 128.

[12] *See infra* Part II.B. for definitions of "personal data" and "processing."

in the European Union.[13] Second, the GDPR applies when a controller or processor is not established in the European Union, but the processing is related to either: the offering of goods or services to European Union residents or monitoring their behavior that takes place within the European Union.[14] Third, the GDPR "applies to the processing of personal data by a controller not established within the [European] Union, but in a place where Member State law applies by virtue of public international law."[15] The GDPR also provides an example for the third application of the GDPR: "such as in a Member State's diplomatic mission or consular post."[16] For most Tennessee businesses, the GDPR will apply when those businesses offer goods or services to European Union residents.

Consumers care about their personal data.[17] United States businesses care about the personal data of European Union residents to deliver data-driven services.[18] The flurry of recent data breaches highlights the need to scrutinize how personal data is handled. In 2016, an Uber data breach revealed the names, email addresses, and phone numbers of 57 million users (along with around 600,000 driver license numbers), and was covered up for a year.[19] In March, 2018, it was discovered that the Facebook-Cambridge Analytica scandal gave access to more than 50 million Facebook users' private information.[20] Cambridge had "tools that could identify the personalities of American voters and influence their behavior."[21] In September 2018, Atrium Health's databases suffered a data breach that exposed the names, addresses, dates of birth, insurance information, medical record numbers, and account balances of more than

---

[13] GDPR, *supra* note 1, art. 3(1). *See infra* Part II.B., for definitions of "controller" and "processor."

[14] *Id.* art. 3(2).

[15] *Id.* art 3(3).

[16] *Id.* recital 25.

[17] J.C. Bruno & Elsa Crozatier, *Compliance with the European Union Directive in the Transfer of Employee Personal Data to U.S. Affiliates*, 83 MICH. B. J. 48, 50 (2004).

[18] Schwartz & Peifer, *supra* note 3, at 117.

[19] Darrell Etherington, *Uber data breach from 2016 affected 57 million riders and drivers*, TECHCRUNCH, (Nov. 21, 2017), https://techcrunch.com/2017/11/21/uber-data-breach-from-2016-affected-57-million-riders-and-drivers/.

[20] *See* Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), http://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

[21] *Id.*

2.6 million patients.[22] Further, the hacker had access to around 700,000 Social Security numbers.[23] These breaches all involved the sort of "personal data" that the GDPR seeks to protect.

The United States and the European Union's approaches to data privacy significantly conflict. The European Union categorizes data privacy rights under a broader, fundamental privacy right.[24] These data privacy rights focus primarily on contract and consent.[25] Contract and consent are further limited to increase the European Union's data privacy protections for data subjects.[26] Contract is limited in European Union data privacy law by necessity, purpose limitation, and prohibiting "tying," or extending, any use of personal data beyond what is necessary for the purpose of the contract.[27] Within the GDPR, consent is subject to a multitude of limitations.[28] Union data privacy law is "strongly anchored at the constitutional level."[29] The United States, on the other hand, "anchors its [data] privacy law in the marketplace."[30] United States consumers freely exchange their personal information within the marketplace, with the government only protecting the consumer when the need arises.[31] This system works well in the United States when it operates transparently, allowing personal data to drive innovation and the digital economy.[32] However, the marketplace exchange, with little to no legal constraints, fails when consumers are no longer involved in the transfer of their personal data. The Federal Trade Commission ("FTC") has questioned the practice of data brokers that collect consumer personal data often without the consumers' knowledge.[33] The FTC reported that "it would be virtually

---

[22] Charlie Osborne, *Atrium Health Data Breach Exposed 2.65 Million Patient Records*, ZDNET (Nov. 28, 2018), https://www.zdnet.com/article/atrium-health-data-breach-exposed-2-65-million-patient-records/.

[23] *Id.*

[24] Schwartz & Peifer, *supra* note 3, at 125, 132.

[25] *Id.* at 120.

[26] *Id.* at 121.

[27] *Id.* at 142—43.

[28] *See infra* Part III.B.

[29] Swartz & Peifer, *supra* note 3, at 127.

[30] *Id.* at 132.

[31] *Id.*

[32] *Id.* at 136—37 (citing WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD 31-32 (Feb. 2012), https://www.hsdl.ord/?view&did=700959).

[33] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 1—2 (May 2014),

impossible for a consumer to determine how a data broker obtained his or her data" and that one data broker "adds three billion new records each month to its databases."[34] With the pervasion of the personal data market and the expansion of data privacy within the GDPR, the conflicts between the European Union's and United States' views on regulating data privacy will remain a focal issue.

B. The General Data Protection Regulation Definitions

Several definitions are important to understanding the GDPR. Article 4 of the GDPR contains the regulation's definitions.[35] "Personal data," as defined by the GDPR, "means any information relating to an identified or identifiable natural person ('data subject'). . . ."[36] The section continues by explaining that:

> an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[37]

Therefore, unless the data is truly anonymous, pseudonymised (explained below), or belonging to a non-natural person (such as a legal entity, like a corporation) the data is likely personal.

"Processing" is "any operation . . . which is performed on personal data . . . whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[38] This extensive list of processing examples likely captures most data operations.

---

https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[34] *Id.* at iv.

[35] GDPR, *supra* note 1, art. 4.

[36] *Id.* art. 4(1).

[37] *Id.*

[38] *Id.* art. 4(2).

"Pseudonymisation," within the GDPR:

> means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identifiable natural person.[39]

Pseudonymised data differs from anonymized data in the GDPR. Anonymized data means data that has been irreversibly altered to not relate to an identifiable natural person.[40] The GDPR does not apply to anonymized data.

Another important distinction is the difference between a "controller" and a "processor" in the context of this regulation. The GDPR defines a controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data . . . ."[41] Processor "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[42]

Lastly, "consent" of an identifiable natural person "means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[43]

C. Privacy Shield

Privacy Shield is an agreement between the United States and the European Union to provide for legal, international transfers of personal

---

[39] *Id.* art. 4(5).

[40] *Id.* recital 26 ("The principles of data protection should therefore 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 loner identifiable. This Regulation does not therefore concern the processing of such anonymous information . . . .").

[41] *Id.* art. 4(7).

[42] *Id.* art. 4(8).

[43] *Id.* art. 4(11).

data.[44] Before Privacy Shield, a privacy agreement called Safe Harbor allowed for data transfers between the United States and the European Union.[45] In 2015, however, the Court of Justice of the European Union invalidated Safe Harbor because it did not comply with the European Union's Data Protection Directive.[46] In response, the parties finalized the European Union-United States Privacy Shield in June 2016. Within the GDPR, Privacy Shield acts as a method of allowing data transfers from the European Union to the United States.[47] Privacy Shield has already faced legal challenges in the European Union, despite its enactment being an attempt to correct the issues encountered under Safe Harbor.[48]

The GDPR only allows transfers to businesses in third countries (including the United States) under three circumstances: binding corporate rules that meet Article 47, standard contractual clauses within Article 46, or the European Commission has decided the third country "ensures an adequate level of protection."[49] Privacy Shield, in the context of the GDPR, acts as a method of determining the adequacy of the decisions allowing data transfers between the European Union and the United

---

[44] Emily Linn, Note, *A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement*, 50 VAND. J. TRANSNAT'L L. 1311, 1313 (2017) (citing Case C-362/14, *Schrems v. Data Protection Comm'r*, 2015 E.C.R. § 106 (holding that the Safe Harbor did not meet the Article 25 requirement for "an adequate level of protection" required to safeguard EU data subject's fundamental right)).

[45] *Id.*

[46] *Id.*

[47]GDPR, *supra* note 1, arts. 44-50; s*ee also* Hayley Evans & Shannon Togawa Mercer, *Privacy Shield on Shaky Ground: What's Up with E.U.-U.S. Data Privacy Regulations*, LAWFARE BLOG (Sept. 2, 2018, 2:31 PM), https://www.lawfareblog.com/privacy-shield-shaky-ground-whats-eu-us-data-privacy-regulations; *GDPR vs Privacy Shield*, PRIVACYTRUST, https://www.privacytrust.com/privacyshield/gdpr-vs-privacy-shield.html (last visited Dec. 12, 2018); Stephan Grynwajc, *Is Privacy Shield GDPR Compliant?*, LAW OFFICE OF S. GRYNWAJC (Mar. 14, 2018), https://www.transatlantic-lawyer.com/2018/03/is-privacy-shield-gdpr-compliant/; David Roe, *Why the Privacy Shield Won't Make You GDPR-Compliant*, CMSWIRE (May 25, 2018), https://www.cmswire.com/information-management/why-the-privacy-shield-wont-make-you-gdpr-compliant/; *The Relationship Between the GDPR and the Privacy Shield for U.S. Organizations*, VERASAFE (Feb. 9, 2018), https://www.verasafe.com/blog/the-relationship-between-the-gdpr-and-the-privacy-shield-for-u-s-organizations/.

[48] Schwartz & Peifer, *supra* note 3, at 119 (citing Peter Sayer, *A Second Privacy Shield Legal Challenge Increase Threat to EU-US Data Flows*, PCWORLD (Nov. 3, 2016 5:05 AM), http://www.pcworld.com/article/3138196/cloud-computing/a-second-privacy-shield-challenge-increases-threat-to-eu-us-data-flows.html).

[49] GDPR, *supra* note 1*,* arts. 45-47.

States.[50] Privacy Shield is not a substitute for compliance with the GDPR.[51] Instead, without Privacy Shield, United States' businesses will have to receive specific authorization directly from the European Commission to lawfully process European Union resident data.[52]

Privacy Shield has key principles that highlight the give-and-take between United States and European Union data privacy values.[53] The first principle is "Notice," which lists information that organizations must provide to individuals before collecting their personal data.[54] Second, "Choice" requires organizations to allow individuals to "opt out" when their personal information is either disclosed to a third party or used for a purpose that is materially different from the purpose that it was originally collected for.[55] Therefore, this "opt out" provision may allow for a change in the use of personal data that is not materially different without the individual's consent.[56] "Accountability for Onward Transfer" places limitations on transfers of personal data to third parties.[57] The "Security" principle requires "organizations creating, maintaining, using or disseminating personal information" to take "reasonable and appropriate measures to protect it . . . taking into due account the risks involved in the processing and the nature of the personal data."[58] The "Data Integrity and Purpose Limitation" principle limits transferring personal data to the extent that it is "relevant for the purposes of processing" and prohibits "incompatible" processing.[59] "Access" gives individuals the right to view their personal data an organization holds and to "be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles."[60] However, the "Access" right is limited when "the burden or expense of providing access would be disproportionate to the risks of the individual's privacy . . . or where the

---

[50] *Id.*

[51] *Id.* arts. 44-50.

[52] *Id.* arts. 44-50.

[53] Schwartz & Peifer, *supra* note 3, at 161.

[54] U.S. DEP'T OF COM., PRIVACY SHIELD FRAMEWORK (2017), https://www.privacyshield.gov/EU-US-Framework [hereinafter PRIVACY SHIELD FRAMEWORK].

[55] *Id.*

[56] Shwartz & Peifer, *supra* note 3, at 163.

[57] PRIVACY SHIELD FRAMEWORK, *supra* note 57.

[58] *Id.*

[59] *Id.*

[60] *Id.*

rights of persons other than the individual would be violated."[61] Lastly, "Recourse, Enforcement and Liability" lists certain mechanisms to ensure compliance with the Privacy Shield Principles, to require prompt response to inquiries relating to Privacy Shield, and to establish liability in the context of an onward transfer.[62]

D. Federal and State Data Privacy Laws Affecting Tennessee Businesses

i. Federal Laws

The United States generally approaches federal data privacy laws by involving itself only when it determines that an industry is in need of regulation.[63] The result is a patchwork of federal laws that affect the way Tennessee businesses handle personal data. The Health Insurance Portability and Accountability Act ("HIPAA") places specific privacy requirements on covered entities and corresponding business associates.[64] The Children's Online Privacy Protection Act ("COPPA") applies to businesses that either use a website directed to children under the age of thirteen, or knowingly collect their personal data.[65] The Gramm-Leach-Bliley Act ("GLBA") requires a privacy notice from businesses that meet

---

[61] *Id.*

[62] *Id.*

[63] Jared Mehre, Note and Comment, *Creating a 21st Century Personal Data Protection Regime in the United States: Consent, Oversight, and Remedial Reform: Lessons from the German Model*, 35 WIS. INT'L L.J. 205, 207 (2017).

[64] Charlotte A. Tshider, *Enhancing Cybersecurity for the Digital Health* Marketplace, 26 ANN. HEALTH L. 1, 10 (2017) (*citing* Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. No. 104-191, 110 Stat. 1938; Health Insurance Technology for Economic and Clinical Health (HITECH) Act of 2009, 42 U.S.C. § 177921 (2016)). Covered entities are: health plans, health care clearinghouses, and a health care provider who transmits any health information in electronic form in connection with a health care transaction. Business associates are people who, on behalf of a covered entity or organized health care arrangement, creates, receives, maintains, or transmits protected health information; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity or organized health care arrangement. The definitions for covered entities and business associates are found in 45 C.F.R. 160.103.

[65] *Symposium Essays from the State of Cyberlaw: Security and Privacy in the Digital Age: In Defense of the Long Privacy Statement*, 76 MD. L. REV. 1044, 1048 (2017) (citing Children's Online Privacy Protection Act of 1998, Pub. L. No, 105-277, 112 Stat. 2681 (codified at 15 U.S.C. §§ 6501-6506 (2012)).

the Act's definition of "financial institution."[66] Under the Fair Credit Reporting Act ("FCRA"), consumer reporting agencies must adopt "reasonable procedures" that help protect a consumer's right to privacy.[67] Other federal laws that impact data privacy in the United States include but are not limited to: Controlling Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act"), the Federal Trade Commission Act, and the Telephone Consumer Protection Act ("TCPA").[68]

ii. Tennessee Laws

Tennessee has put into place its own matrix of state laws affecting how businesses approach data privacy within the state. Primarily, Tennessee has enacted Tennessee Code Annotated § 47-18-2107, which requires:

> Following discovery or notification of a breach of system security by an information holder, the information holder shall disclose the breach of system security to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement . . . .[69]

At the time it was enacted, Tennessee's breach notification law was groundbreaking.[70] Before Tennessee amended its breach notification statute, most states did not require notification of a breach when the data was adequately encrypted.[71] In 2016, Tennessee was the first state to potentially require notification of a breach even if the data was encrypted.[72]

Supporters of the GDPR most likely find Tennessee's definition for "personal information" too lack luster in comparison to the GDPR's

---

[66] *Id.* (citing 15 U.S.C. §§ 6801-6809 (2012).

[67] Fair Credit Reporting Act, 15 U.S.C. § 1681 (2003).

[68] Federal Trade Commission Act, 15 U.S.C. § 45 (2006); Telephone Consumer Protection Act, 47 U.S.C. § 227 (1991); Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. § 7701.

[69] TENN. CODE ANN. § 47-18-2107 (2016).

[70] Shawn E. Tuma, *Understanding Basic "Data Breach" Foundations*, 2016 TXCLE-ABL 4.III (2016).

[71] *Id.*

[72] *Id.*

broad "personal data" definition. Under Tennessee law, "personal information" means "an individual's first name or first initial and last name" together with either a social security number, driver's license number, and account or credit card number (with its security code).[73] It is easy to envision the sorts of personal information that fall within the GDPR, but not Tennessee's Breach Notification Law. Those that oppose the broad reach of the GDPR would likely find the Tennessee definition as a paradigm for the sort of information that deserves protection.

Other laws that impact data privacy in Tennessee include Tennessee Compilation of Rules and Regulations §§ 0780-01-72-.11, 0780-01-72-.12, and 0780-01-72-.13.[74] These regulations place limits on disclosure of nonpublic personal information to nonaffiliated third parties, redisclosure and reuse of nonpublic personal information, and sharing account number information for marketing purposes.[75] Tennessee has also enacted the Video Consumer Privacy Act, which protects consumer privacy in regards to rented video and audio.[76] Tennessee businesses must therefore comply with federal, state, and potentially foreign data privacy laws.

iii. Other State Laws

Lastly, Tennessee businesses may need to comply with other states' privacy laws. For example, California, one of the leaders in the United States on data privacy laws, has two important statutes to note (and one more that will take effect in 2020).[77] The California Data Breach Notification Law can be found in Cal. Civ. Code § 1798.82.[78] The California Data Breach Notification Law requires:

> A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach… to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is

[73] TENN. CODE ANN., *supra* note 41.
[74] TENN. COMP. R. & REGS, 0780-01-72-.11, 0780-01-72-.12, and 0780-01-72-.13 (2001).
[75] *Id.*
[76] TENN. CODE ANN. §§ 47-18-2201-2205 (1999).
[77] *See infra* Part IV.A. for a discussion on the California Consumer Privacy Act.
[78] CAL. CIV. CODE § 1798.82 (West 2016).

> reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable.[79]

Therefore, Tennessee businesses that conduct business in California must follow the California Data Breach Notification Law when a breach of a California resident's personal data occurs. California also has the California Online Privacy Protection Act, which mandates that operators of a commercial website or online service that collects personal data online about California residents who use or visit the website or online service post a privacy policy.[80] Other states also have their own data privacy laws, and Tennessee businesses must comply with those laws if they conduct business in or collect personal data from residents of those states.

III. The General Data Protection Regulation

A. The Principles and Rights

The GDPR articulates the principles for personal data in Article 5.[81] It states that personal data shall be: (1) "processed lawfully, fairly, and in a transparent manner,"(2) "collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes," (3) "adequate, relevant and limited to what is necessary" for those purposes (data minimisation), (4) accurate (5) stored in a manner that ensures identification of data subjects is limited to what is necessary, and (6) given appropriate security. Article 5 goes on to place the responsibility for compliance with these principles on the controller.[82]

These principles show the essential goals of the GDPR. The GDPR makes these principles actionable; however, some of them may be more idealistic than realistic. They explicitly note the goal to have personal data processed in a transparent manner.[83] Supporters of the GDPR likely believe there has been a dire need for this principle to be actionable, as evidenced by the recent Facebook-Cambridge Analytica scandal.[84] While

---

[79] *Id.*

[80] CAL. BUS. & PROF. CODE § 22575 (West 2013).

[81] GDPR, *supra* note 1, art. 5.

[82] *Id.*

[83] *Id.*

[84] Granville, *supra* note 20.

the realm of data privacy will likely never truly be private or transparent, this principle appears to be a good stepping-stone towards preventing these sort of shady practices. Asking for "specified, explicit" purposes for processing personal data lays the groundwork for pursuing those breaking the first principle.[85] These specified and explicit purposes should be "determined at the time of the collection of the personal data."[86] Data minimisation requires "ensuring that the period for which the personal data are stored is limited to a strict minimum."[87] Lastly, the requirement that a *controller* has responsibility for showing compliance with the principles is important to note.[88] While processors do have direct obligations, controllers have a heavier burden throughout the GDPR.[89]

The GDPR also gives certain rights to data subjects. The controller of personal data has the obligation to "facilitate the exercise of data subject rights under Articles 15 to 22."[90] These rights are the right of access, right to rectification, right to erasure, right to restriction of processing, right to data portability, and the right to object.[91]

The right to access gives a data subject the right to access certain information regarding his or her personal data from the controller.[92] That information includes: the "purposes of processing," the "categories of personal data concerned," the "recipients or categories of recipient to whom the data have been or will be disclosed," the period for which the personal data will be stored or the criteria to determine that period, the "existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing," the right to submit a complaint to a supervisory authority, the source of the personal data when the data is not collected from the data subject, and the "existence of automated decision-making."[93] Further the right of access asks the controller to, where possible, "provide remote access to a secure system which would provide the data subject with direct access to his or

---

85 GDPR, *supra* note 1, art. 5.
86 *Id.* recital 39.
87 *Id.* recital 39.
88 *Id.* art. 5(2).
89 *Id.* art. 4 (defining "controller" and "processor").
90 *Id.* art. 12(2).
91 *Id.* arts. 15–21.
92 *Id.* art. 15.
93 *Id.* art. 15(1).

her personal data."[94] The right of access "should not adversely affect the rights or freedoms of others . . . [h]owever, the result of those considerations should not be a refusal to provide all information to the data subject."[95]

The right to rectification gives data subjects the "right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her."[96]

The right to erasure (also known as "the right to be forgotten") allows the data subject to have his or her personal data erased by the controller without undue delay when one of the following occurs: (1) "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;" (2) consent by the data subject is withdrawn; (3) there are no longer legitimate grounds for processing under Article 21; (4) "the personal data have been unlawfully processed"; (5) erasure is required "for compliance with a legal obligation in Union or Member State law"; or (6) "the personal data have been collected in relation to an offer of information society services" directed towards a child.[97] The right to erasure does not apply when processing is necessary to exercise "the right of freedom of expression and information," to comply with a legal obligation, to perform a task carried out in the public interest, to exercise official authority vested in the controller, to promote a public interest in health, to archive "purposes in the public interest, [to further] scientific or historical research purposes or statistical purposes, or [to promote] the establishment, exercise or defence [sic] of legal claims."[98]

The right to restriction of processing allows data subjects to restrict a controller's processing when the following occurs: the data subject contests the accuracy of the personal data, the processing is unlawful, "the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence [sic] of legal claims," or the data subject objects to

[94] *Id.* recital 63.

[95] *Id.*

[96] *Id.* art. 16.

[97] *Id.* art. 17. *See infra* Part III.B. for a discussion on the unlawful processing of personal data.

[98] *Id.* recital 65.

processing pursuant to Article 21.[99] Recital 67 lists examples showing how to restrict the processing of personal data in accordance with Article 18.[100]

The right to data portability gives the data subject the right to "receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format" and transmit that data to another controller when either the processing is carried out by automated means or the processing is based on consent or contract.[101] The processing of European Union residents' data for many businesses will be made lawful by consent or contract, and, in that event, this right will apply.

When the processing of personal data is made lawful either by necessity to perform a task "carried out in the public interest or in the exercise of official authority vested in the controller" or by necessity for the "purposes of the legitimate interests pursued by the controller or by a third party," the data subject has the right to object to the processing.[102] At that time, the controller can no longer process the personal data "unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence [sic] of legal claims."[103] The data subject also has the right to object when the personal data are processed for direct marketing purposes.[104]

B. Compliance

The GDPR applies to Tennessee businesses that process personal data of European Union residents when the processing is related to either "the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects . . . or the monitoring of their behavior as far as their behavior takes place within the Union."[105] When the GDPR applies to controllers or processors not established in the European Union, they must designate in writing a representative in the European Union.[106] Therefore, Tennessee controllers or processors who

---

[99] *Id.* art. 18.
[100] *Id.* recital 67.
[101] *Id.* art. 20.
[102] *Id.* art. 21.
[103] *Id.*
[104] *Id.*
[105] *Id.* art. 3.
[106] *Id.* art. 27.

are subject to the GDPR for offering goods or services or monitoring behavior within the European Union must designate this representative, except when the "processing is occasional, does not include, on a large scale, processing of special categories of data . . . or processing of personal data relating to criminal convictions and offences . . . and is unlikely to result in a risk to the rights and freedoms of natural persons . . . ."[107]

The GDPR has lengthy requirements for the lawful processing and use of personal data of data subjects located in the European Union. Article 6 lists the requirements to process data lawfully.[108] Methods of lawful processing under Article 6 include: consent, necessity to perform a data subject's contract, legal obligation of the controller, protection of the "vital interests" of a natural person, performance of a public interest task or exercise of official authority, or "legitimate interests of the controller or third party.[109] Most businesses will likely use the "consent" or "contract" requirement to comply with the GDPR.

Major websites that collect personal data have already been updated to ask for consent to collect such information. Article 7 defines the conditions for consent: (1) the controller shall demonstrate that a data subject has given consent to the processing of his or her personal data; (2) if consent is given in a writing that concerns other matters, the request for consent shall be distinguishable from the other matters in clear and plain language; (3) consent can be withdrawn at any time in a manner that is as easy as it is to give consent, and the data subject should be told this right prior to giving consent; and(4) in determining if consent is freely given, it will be considered whether performance of a contract, "including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[110] Consent cannot be informed unless the data subject is aware of "at least the identity of the controller and the purposes of the processing for which the personal data are intended."[111] Further, "if that data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive

107 *Id.*

108 *Id.* art. 6.

109 *Id.*

110 *Id.*

111 *Id.* recital 42.

to the use of the service for which it is provided."[112] Consent is not freely given if "the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."[113]

Businesses may also use contract for lawful processing.[114] The Information Commissioner's Office ("ICO"), the United Kingdom's supervisory authority, provides a helpful explanation of using contract for lawful processing—"when a data subject makes an online purchase, a controller processes the address of the individual in order to deliver the goods. This is necessary in order to perform the contract."[115]

The controller has the responsibility to provide any information required by Article 13 or 14 and any communication from Articles 15 to 22.[116] This information must be provided without undue delay and "in any event within one month of receipt of the request."[117]

Article 13 requires controllers to provide notices to data subjects ("Article 13 Notices") when personal data are obtained.[118] Article 13 Notices must include the identity and contact details of the controller, the contact details of the data protection officer, the purposes and legal basis for the processing, "the recipients or categories of recipients of the personal data," the intent to transfer personal data to a third country or international organization, "the existence or absence of an adequacy decision by the Commission," the period personal data will be stored "or if that is not possible, the criteria used to determine that period," the existence of the GDPR rights, the right to lodge a complaint with a supervisory authority, and the existence of automated decision-making.[119] When the personal data is collected from someone other than the data subject, Article 14 requires controllers to provide notices to the data subjects ("Article 14 Notices") that are as extensive as Article 13 Notices.[120] Article 14 Notices require the same information as Article 13

---

112 *Id.* recital 32.

113 *Id.* recital 43.

114 *Id.* art. 6.

115 INFORMATION COMMISSIONER'S OFFICE, GUIDE TO THE GENERAL DATA PROTECTION REGULATION: CONTRACT, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/ (last visited Dec. 14, 2018).

116GDPR, *supra* note 1, art. 12(3).

117 *Id.*

118 *Id.* art. 13.

119 *Id.*

120 *Id.* art. 14.

Notices, as well as the source where the personal data originates and "whether it came from publicly accessible sources."[121] The bulk of these Notices recite the information protected by the right to access.[122]

The controller also has the responsibility to "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the GDPR]."[123] The GDPR tasks controllers with employing "data protection by design and by default," which mandates that the controller, "both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures . . . which are designed to implement data-protection principles . . . in an effective manner and to integrate the necessary safeguards into the processing . . ." to comply with the GDPR.[124]

Controllers must also maintain a record of processing activities under its responsibility.[125] Processors, in turn, must maintain a record of all processing activities performed on behalf of a controller.[126] The specific requirements of these records are found in Article 30.[127] Controllers and processors with less than 250 employees do not have to keep these records unless the processing "is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or data on criminal convictions and offenses."[128]

Controllers must alert data subjects of a personal data breach "without undue delay and, where feasible, not later than 72 hours after having become aware of it . . . unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."[129] Processors must notify controllers of a personal data breach without undue delay.[130]

Processing by a processor must be governed by a contract or other legal act under Union or Member State law that is binding on the

---

121 *Id.* arts. 13-14.
122 *Id.* art. 15.
123 *Id.* art. 24(1).
124 *Id.* art. 25.
125 *Id.* art. 30.
126 *Id.*
127 *Id.*
128 *Id. See supra* Part III.A for discussion of data subject's rights.
129 *Id.* art. 33.
130 *Id.*

processor.[131] The contract or other legal act must set out that the processor processes only on documented instructions from the controller, promises to have persons authorized to process the personal data committed to confidentiality, takes all security of processing measures laid out in Article 32, respects conditions for engaging other processors, assists the controller in responding to requests arising out of data subject rights, assists the controller in complying with obligations found in Articles 32 through 36, deletes or returns all of the personal data to the controller, and makes all information needed to demonstrate compliance with Article 28 available to the controller.[132] Further, processors cannot "engage another processor without prior specific or general written authorisation of the controller."[133] If a processor violates the GDPR by "determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing."[134] Therefore, the processor would be subject to the larger responsibilities of the controller in those situations.

The data protection officer largely ensures that the controller or operator complies with the GDPR, and a list of minimal duties that can be found in Article 39.[135] Controllers and processors will need to designate a "data protection officer" when: the processing is performed by a public authority or body, "the core activities of the controller or processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale," or the activities consist of processing on a large scale special categories of data or "personal data relating to criminal convictions and offenses."[136] Multiple "undertakings" may use a single data protection officer so long as the data protection officer is "easily accessible from each establishment."[137] The data protection officer cannot be penalized or discharged for performing his job and reports to the "highest management level of the controller or processor."[138]

131 *Id.* art. 28.
132 *Id.*
133 *Id.*
134 *Id.*
135 *Id.* art. 39.
136 *Id.* art. 37.
137 *Id.*
138 *Id.* art. 38.

Noncompliance with the GDPR could lay a heavy toll on any business. United States businesses can be fined by the GDPR through international law.[139] Further, Privacy Shield put in place a system to allow the European Union to fine United States businesses.[140] The GDPR authorizes fines and other penalties for infringements of the Regulation.[141] The GDPR uses a tiered approach on punishment that imposes more significant fines on more significant violations.[142] Each Member State is required to establish supervisory authorities that are responsible for applying the Regulation, as well as imposing fines and other penalties.[143]

When considering the amount of the fine, the GDPR says to consider "the nature, gravity and duration of the infringement . . . as well as the number of data subjects affected and the level of damage suffered by them," whether the infringement was intentional or negligent, actions to mitigate the damage, the degree of responsibility of the controller or processor, relevant previous infringements, cooperation with the supervisory authority, categories of personal data affected, whether the controller or processor notified the supervisory authority of the infringement, whether other measures beyond fines had been previously taken, and "any other aggravating or mitigating factor applicable to the circumstances."[144] Lesser offenses, namely noncompliance, with the obligations of the controller and processor under Articles 8, 11, 25 to 39, 42 and 43, are subject to fines up to €10,000,000 ($11,341,920 at the time of writing) or 2% of the total worldwide annual turnover (gross revenues) of the preceding financial year, whichever is higher.[145] For violations of core GDPR principles in Articles 5-7 and 9, data subjects rights in Articles 12-22, or rules for transferring to a recipient in a third country or international organization under Articles 44 to 49, the fines can reach €20,000,000 ($22,689,240) or 4% of the total worldwide annual turnover from the previous financial year, whichever is higher.[146]

---

139 PRIVACY SHIELD FRAMEWORK, *supra* note 53.

140 *Id.*

141 GDPR, *supra* note 1, art. 84. *See also id.* recital 148.

142 *Id.* art 83.

143 *Id.* arts. 51, 83.

144 GDPR, *supra* note 1, art. 83.

145 *Id.*

146 *Id.*

C. Beginnings of Case Law

While the GDPR is still new, case law interpreting it is beginning to appear overseas and in the United States. In Germany, the Internet Corporation for Assigned Named and Numbers ("ICANN") sought to require Registrar EPAG Domainservices GmbH ("EPAG") to comply with ICANN's "Registrar Accreditation Agreement."[147] The Agreement asks that registrars collect administrative and technical contact information for a domain name registration.[148] The court held that the collection of this data is not necessary per Article 5, and therefore EPAG was not obligated to collect this data within the GDPR.[149] The decision was supported by the fact that registration could occur by listing the registrant, rather than a third party as the administrative and technical contacts.[150] This ruling shows how the European courts, or at least German courts, may interpret the GDPR when it comes to "specified, explicit and legitimate purposes" and the "adequate, relevant and limited" collection. This holding lies on the side of protecting data subjects, and allows less information to be collected by necessity. Further, this may limit the "legitimate interests" allowed for lawful processing under Article 6, and require more controllers to rely on consent which can easily be withdrawn at anytime by the data subject.

In the United States, *Corel Software, LLC v. Microsoft Corp.* discussed discovery of information subject to the GDPR.[151] Microsoft argued that its "telemetry data" retention of which would require anonymization to comply with the GDPR.[152] The court essentially ignored this argument and denied Microsoft's motion for a protective order.[153] This case highlights that compliance with the GDPR will not replace responsibilities within the United States.

---

147 Jan Spittka and Kiana Mirzaei, *Germany: First Court Decision on GDPR*, DLA PIPER: PRIVACY MATTERS, (June 6, 2018), https://blogs.dlapiper.com/privacymatters/germany-first-court-decision-on-gdpr/ (discussing LGB, May 29, 2018, 10 O 171/18, https://www.icann.org/de/system/files/files/litigation-icann-v-epag-request-court-order-prelim-injunction-redacted-30may18-de.pdf).

148 *Id.*

149 *Id.*

150 *Id.*

151 *Corel Software, LLC v. Microsoft Corp.*, No. 2:15-cv-00528-JNP-PMW, 2018 U.S. Dist. LEXIS 172875, at *3-8 (D. Utah, Oct. 5, 2018).

152 *Id.* at *3.

153 *Id.* at * 7-8.

A German supervisory authority imposed its first GDPR fine of €20,000 on a social media provider following a data breach that exposed the personal data of around 330,000 users.[154] The company's cooperation with the supervisory authority helped mitigate a larger fine.[155] France's data protection authority, the Commission Nationale de l'Informatique et des Libertes ("CNIL"), levied a €50,000,000 fine against Google for "forced consent," a lack of transparency, and inadequate information.[156] Additional high profile cases against Google, Facebook, Instagram, and WhatsApp are in the preliminary stages.[157] Twitter is also being investigated for infringing the GDPR.[158] These cases will be revealing of how harshly fines will be levied against companies that violate the GDPR.

D. Criticism

i. GDPR and Competition

The GDPR has also been accused of protecting larger companies while hampering the ability of smaller businesses to grow.[159] This would lead to stifling both competition and innovation.[160] Federal Trade Commissioner Phillips explains that the "economies of scale" allow larger companies to bear the compliance costs required to comply with the GDPR more easily than smaller businesses can.[161]

---

154 Henrik Hanßen & Stefan Schuppert, *Data Protection Authority of Baden-Württemberg Issues First German Fine Under the GDPR*, JD SUPRA (Nov. 26, 2018), https://www.jdsupra.com/legalnews/data-protection-authority-of-baden-11482/.

155 *Id.*

156 Glyn Moody, *Google Hit with First Big GDPR Fine Over "Forced Consent'; Eight New Complaints Filed Over "Right to Access"*, PRIVACY NEWS ONLINE (Feb. 2, 2019), https://www.privateinternetaccess.com/blog/2019/02/google-hit-with-first-gdpr-fine-over-forced-consent-eight-new-complaints-filed-over-right-to-access/.

157 Foo Yun Chee, *EU Privacy Chief Expects First Round of Fines Under New Law by Year-End*, REUTERS (Oct. 9, 2018, 1:58 PM), https://www.reuters.com/article/us-eu-gdpr-exclusive/exclusive-eu-privacy-chief-expects-first-round-of-fines-under-new-law-by-year-end-idUSKCN1MJ2AY

158 David Meyer, *Twitter Under Formal Investigation for How It Tracks Users in the GDPR Era*, FORTUNE (Oct. 12, 2018), http://fortune.com/2018/10/12/twitter-gdpr-investigation-tco-tracking/

159 Noah Joshua Phillips, Comm'r, Fed. Trade Comm'n, Address at the Internet Governance Forum USA: Keep It: Maintaining Competition in the Privacy Debate (July 27, 2018) (2018 WL 3655792).

160 *Id.*

161 *Id.*

While it is true that most large businesses can afford those costs imposed by the GDPR more easily than small businesses, the costs that the GDPR imposes are unlikely to stymie growth of small businesses for three reasons. First, new or small businesses that are subject to the GDPR and plan at an earlier stage can be better prepared to comply with the GDPR. For example, large companies that have stored data a certain way for years and keep various fragments of one data subject's personal data stored separately will have a more difficult time complying with the right to erasure or the right to portability than a new company that prepares for this on the front-end. Second, many of the costs will be to scale, and at any earlier stage in a business the costs to comply with the GDPR will be less. For instance, a large business may need a dedicated Data Protection Officer whose sole job it is to fulfill the requirements of the GDPR because it controls or processes a huge amount of information. Meanwhile, a smaller business that does not control or process as much information can have this position filled by an officer that works in its IT or legal departments, as explicitly allowed by the GDPR's Article 38.[162] Lastly, the GDPR specifically addresses that "micro, small and medium-sized enterprises" have different needs in comparison to large businesses.[163] The GDPR provides organizations with fewer than 250 employees an exemption to the record-keeping requirement, and encourages "the Union institutions and bodies, and Member States and their supervisory authorities . . . to take account of the specific needs of micro, small, and medium-sized enterprises in the application of [the GDPR]."[164] Therefore, the GDPR should not hurt either competition or innovation to the degree that it has been criticized.

ii. GDPR and Blockchain

The GDPR has been criticized as being incompatible with one of the hottest developments in the data tech world: blockchain.[165] In an extremely

---

[162] GDPR, *supra* note 1, at art. 38 ("The data protection officer may fulfill other tasks and duties").

[163] *Id.* recital 13.

[164] *Id. See supra* Part III.B. (addressing the derogation for micro, small, and medium-sized enterprises).

[165] David Pollock, *How Can Blockchain Thrive in the Face of European GDPR Blockade?*, FORBES (Oct. 3, 2018, 4:07 AM), https://www.forbes.com/sites/darrynpollock/2018/10/03/how-can-blockchain-thrive-in-the-face-of-european-gdpr-blockade/#4368dea461df.

simplified definition, blockchain is a digital and decentralized database that records every transaction that occurs within it. Blockchain and the GDPR are, on their face, compatible in some regards. For one, the GDPR asks for data subjects to have control of their data and the ability to access it at any time. Meanwhile, blockchain has a similar goal of offering transparency in the data it records.[166] However, while the GDPR and blockchain are compatible in ideals, they conflict in almost every way in practice. Blockchain is immutable in nature, which hinders two key rights of data subjects under the GDPR: the right to rectification, and the right to be forgotten. The French CNIL has begun to analyze how the GDPR and blockchain technology can work together.[167] The initial release of the French CNIL's analysis acknowledges the challenges to allowing a decentralized technology like blockchain to work under the GDPR.[168] More importantly, the analysis illustrates that privacy authorities within the European Union consider blockchain technology to be within the GDPR's grasp.[169]

One solution to the GDPR-blockchain clash is to pseudonymize the personal data with an encrypted key acting as a unique identifier.[170] Once a controller has the key, it can identify the data subject and processing of that data becomes subject to the GDPR. If a data subject requests the erasure of their data, the controller could just delete the key. There are two other potential solutions: (1) anonymize the data, or (2) avoid recording personal data into the blockchain.[171] Anonymizing personal data that does not need identification to particular data subjects would relieve a need to prepare for the right to erasure.

iii. Right to be Forgotten

Some argue that the GDPR simply will not work with the United States' form of data privacy, especially in regards to the conflict between

---

166 *Id.*

167 Laura Jehl, Robert Musiala, & Stephanie Malaska, *French Guidance Takes First Steps Applying GDPR to Blockchain*, BLOOMBERG L.: PRIVACY & DATA SECURITY (Oct. 29, 2018), https://www.bna.com/insight-french-guidance-n57982093336/.

168 *Id.*

169 *Id.*

170 Bruce Bennett et al., *The GDPR and Blockchain*, COVINGTON: INSIDE PRIVACY (July 24, 2018), https://www.insideprivacy.com/international/european-union/the-gdpr-and-blockchain/

171 *Id.*

the GDPR's "Right to be Forgotten" and the United States' First Amendment.[172] Essentially, they may not be able to work together because one cannot force another to erase personal information after it's posted if the poster is exercising his or her freedom of speech. However, this conflict may not truly exist, and it will not be certain until clarification by the European Union or the courts enforcing the GDPR. The GDPR built in an exception to the right to erasure in the GDPR's Article 17: "[the right of erasure] shall not apply to the extent that processing is necessary . . . for exercising the right of freedom of expression and information . . . ."[173] This might imply a difference between treatment of a data subject's personal data and information shared through the freedom of speech. Article 85 specifically states, "Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression."[174] For example, an article written about the Chancellor may not be subject to the right to erasure because the Chancellor did not provide personal data, but instead the author created the article through her freedom of speech. Personal data in the GDPR is any information relating to an identifiable natural person, and any information that might be included in the article would constitute personal data within the meaning of the GDPR. The GDPR does not further explain this exception, and it will be interesting to see this how case law develops it.

iv. Does the GDPR Go Too Far?

Many criticize the GDPR as going too far. For example, in the *ICANN* case (see Part III.C, *supra*) the Agreement requests the administrative and information contact information for domain registration. The court's holding that the information was not required because it was not necessary under the GDPR highlights an issue some see in the GDPR.

One criticism that the GDPR imposes too much is the vast amount of compliance required. These requirements include hiring a data protection officer, reporting a data breach within 72 hours, and ensuring

---

[172] Max Read, *The E.U.'s New Privacy Laws Might Actually Create a Better Internet*, NY MAG: INTELLIGENCER (May 15, 2018), http://nymag.com/intelligencer/2018/05/can-gdpr-create-a-better-internet.html.

[173] GDPR, *supra* note 1, at art. 17.

[174] *Id.* art. 85.

the data subject's rights can be facilitated.[175] These requirements place a huge burden on controllers, especially within smaller companies. Some might argue that the requirements imposed should already be in place when a business processes personal data. However, it is apparent that adapting to the GDPR compliance structure will take time and money.

Another issue is whether the "intrusion" of increased government power can work with United States' privacy law.[176] Critics argue that selective enforcement could "produce bias, corruption, and prejudice,"[177] however, selective enforcement is an issue with any law. The problem lies in the enforcement rather than the law itself. Further, a law that fosters transparency would hopefully curtail selective enforcement.

The GDPR does overstep United States' privacy norms. It places a heavy burden on business for compliance and introduces inherent threats. However, the regulatory framework allows for greater protection of individual data privacy rights and creates actionable conduct for dishonest business practices. The implementation of the GDPR represents a view on privacy in the European Union that the United States has not yet protected.

IV. The Future for Tennessee Data Privacy Law

A. Developments in the United States

Several states have begun to implement new data privacy laws which show the newfound importance of data privacy in light of the GDPR. The most comprehensive of these laws is the California Consumer Privacy Act of 2018.[178] The law goes into effect on January 1, 2020, and while it does not perfectly mirror the GDPR, this "GDPR-lite" shows that the state is considering the data privacy issues that the GDPR highlights. The law gives California residents four rights: (1) the right to know what personal data regarding them a business collects, where it was sourced, why it is being used, and to whom it is disclosed or sold; (2) the right to opt out of allowing their personal data to be sold to third parties; (3) the

---

175 Seth Berman, *GDPR in the U.S.: Be Careful What You Wish For*, GOVERNMENT TECHNOLOGY (May 23, 2018), http://www.govtech.com/analysis/GDPR-in-the-US-Be-Careful-What-You-Wish-For.html.

176 Roslyn Layton & Julian Mclendon, *The GDPR: What it Really Does and How the U.S. Can Chart a Better Course*, 19 FEDERALIST SOC'Y REV. 234, 236 (2018).

177 *Id.* at 240.

178 Assemb. B. 375, 2017 Assemb., Reg. Sess. (Cal. 2018).

right to have their personal data deleted (with exceptions); and (4) the right to receive equal service and pricing, regardless of whether they exercise their privacy rights.[179] The new law applies to any for-profit businesses that collect and control the personal data of California residents, conduct business in California, and: "(a) have annual gross revenues in excess of $25 million; or (b) receive or disclose the personal information of 50,000 or more California residents, households or devices on an annual basis; or (c) derive 50 percent or more of their annual revenues from selling California residents' personal information."[180]

Other states have also begun to improve upon their data privacy laws. For example, Alabama and South Dakota recently passed the first data breach notification laws of their respective states.[181] Colorado updated its data privacy law to require certain data protection policies that mimic the sentiment found in the GDPR.[182] Nebraska now requires "an individual or commercial entity that conducts business" within the state and "owns, licenses, or maintains" personal data of Nebraska residents to implement "reasonable security procedures and practices that are appropriate to the nature and sensitivity of the personal information . . . ."[183] It also mandates that an individual or commercial entity that discloses personal data of Nebraska residents to a third party must require "by contract" that the third party implement and maintain reasonable security procedures and practices.[184] Vermont passed new legislation that will require data brokers that operate within the state and collect information about Vermont residents to register annually with the Vermont Secretary of State, and to "provide information about the data collection activities, opt-out policies, purchaser credentialing practices, and security breaches."[185]

On the other hand, Ohio has enacted the "Data Protection Act" which provides a legal safe harbor to businesses from data breach suits if an individual has a cybersecurity program that meets the requirements of the

---

[179] Kristen J. Mathews & Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, PROSKAUER: PRIVACY L. BLOG (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/

[180] *Id.*

[181] S.B. 318, 2018 S., Reg. Sess. (Ala. 2018); S.B. 62, 93rd Legis. Assemb., 2018 (S.D. 2018).

[182] H.B. 1128, 71st Gen. Assemb., 2d Reg. Sess. (Colo. 2018).

[183] Legis. B. 757, 105th Leg., 2d Reg. Sess. (Neb. 2018).

[184] *Id.*

[185] H.B. 764, 2017 H., Legis. Sess. (Vt. 2018).

Act.[186] The Act gives two situations where a business has enacted an appropriate cybersecurity program. First, the business can meet substantial compliance with the National Institute of Standards and Technology's ("NIST") special publication 800-171, NIST special publication 800-53 and 800-53a, the federal risk and authorization management program, the Center for Internet Security Critical Security controls, or the International Organization for Standardization/International Electrotechnical Commission 27000 series.[187] Second, if the state and the federal government regulate the business, it has an appropriate cybersecurity program in place if: it is in substantial compliance with the security requirements of HIPAA, Title V of the Gramm-Leach-Bliley Act (as amended), or the Federal Information Security Modernization Act of 2014.[188] If the business implements an appropriate cybersecurity framework, the business can plead safe harbor as an affirmative defense in a data breach suit.[189] The Act "is intended to be an incentive and to encourage businesses to achieve a higher level of cybersecurity through voluntary action."[190] Further, the Act "does not, and is not intended to, create a minimum cybersecurity standard . . . ."[191]

The United States federal government has also taken some actions that suggest a move towards a more GDPR-compliant regime. United States Senate Resolution 523 asks that entities covered by the GDPR provide "people of the United States" with the same privacy protections afforded in the GDPR, "in a manner consistent with existing laws and rights in the United States, including the First Amendment . . . ."[192] While it is unlikely that it will pass (it is currently sitting in the Committee on Commerce, Science, and Transportation), it shows that some legislators want to extend the GDPR's broad data privacy protections for European Union residents to United States "people."

However, with a federal data privacy bill comes the possibility of preemption. A preempting federal data privacy law that does not meet the standard set by California's GDPR-lite would impair the rights of over 39 million U.S. citizens. Therefore, any federal data privacy with preemption

186 S.B. 220, 132nd Gen. Assemb., Reg. Sess. (Ohio 2018).
187 *Id.*
188 *Id.*
189 *Id.*
190 *Id.*
191 *Id.*
192 S. Res. 523, 115th Cong. (2018).

should work carefully to ensure adequate protection as society moves online.

B. Revolutionizing Data Privacy in Tennessee

It is reasonable to believe that Tennessee may join California as a leader in revolutionizing state data privacy law. Remember, Tennessee was at the forefront of requiring notification of a breach regardless if the data was encrypted.[193]

Tennessee legislators introduced Tennessee House Bill 2508 to improve the deficiencies in Tennessee Code Annotated § 47-18-2107.[194] It amends the definition of personal information to include:

> A government issued driver license or identification number, including a federal employer or taxpayer identification number; a passport number; a username or email address, in combination with a password or security question and answer that would permit access to an online account; medical information; health insurance information; unique biometric data generated from measurement or analysis of human body characteristics for authentication purposes; and password protected digital photographs or digital videos not otherwise available to the public.[195]

This would bring the Tennessee definition of "personal data," in the context of our breach notification law, much closer to the GDPR's definition of "personal data."[196] The amendment goes on to detail changes on notifying and cooperation between the information holder and the owner or licensee.[197] While this amendment was deferred and failed after the executive deadline passed, it still represents changes that Tennessee legislators are considering and would make Tennessee law more in line with the GDPR.[198]

Tennessee might find success if it chose to enact a law like California's that brings it closer to GDPR compliance. In doing so, it would help protect the state's small, medium, and large businesses that offer goods or services to European Union residents from noncompliance with the

193 Tuma, *supra* note 9.

194 2017 Legis. Bill Hist. TN H.B. 2508 (Lexis 2017).

195 *Id.*

196 *Id.*

197 *Id.*

198 2017 Bill Tracking TN H.B. 2508 (Lexis 2018).

GDPR. Further, if Tennessee included a provision similar to the safe harbor provided in Ohio's Data Protection Act, it could not only encourage these businesses to comply with a more expansive data privacy law, but also attract businesses to Tennessee. There may be some concern with a safe harbor for data privacy violations given the lack of transparency that currently exists. Therefore, a safe harbor provision should be carefully tailored to balance the need to incentivize businesses to amp up their data privacy protections with the need to hold businesses accountable for failing to protect personal data. The safe harbor would not prevent businesses from being sued for failing to follow other data privacy rules (the safe harbor would only protect data breach suits) or subjected to GDPR fines and penalties. The GDPR would still apply when Tennessee businesses offer goods or services to European Union residents. However, the safe harbor would give incentive, as the Ohio Act indicates, to voluntarily adopt appropriate cybersecurity measures to receive protection from data breach suits in Tennessee. Tennessee courts could help foster compliance with data privacy rules by using injunctions instead of burdensome fines. By adopting a GDPR-lite type of data privacy law and a soft-touch transitional period for penalties, Tennessee could prepare its businesses for the international data privacy regulations. Lastly, this would not only attract businesses dealing directly with data, but international businesses of all types that may wish to benefit from: (1) data privacy laws that would prepare them for the GDPR, (2) soft-touch guidance from the courts, and (3) safe harbor from data breach suits. Therefore, a large reform to Tennessee's current data privacy laws would benefit and attract business in the state.

V. Conclusion

Many view the GDPR as a gold standard for data privacy protections. The United States and the European Union engage in "the largest cross-border data flow in the world."[199] Tennessee businesses that collect personal data of European Union residents must comply with the GDPR or will they be subject to burdensome fines. The United States may never enact a federal data privacy law like the GDPR; however, Tennessee could potentially do so. While the GDPR seems extreme to some in the United States, it represents a sentiment of personal ownership of one's data in the European Union. As time goes on and the world becomes more and more

[199] Linn, *supra* note 44.

entrenched online, the GDPR-based sentiment is likely to continue spreading throughout the United States. Consequently, Tennessee businesses should prepare for compliance as GDPR-like regulations spread across the country and the globe.