American Business Law Journal
ACADEMY OF LEGAL STUDIES IN BUSINESS

American Business Law Journal
Volume 56, Issue 2, 287–344, Summer 2019

Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies

W. Gregory Voss and Kimberly A. Houser***

The European Union's General Data Protection Regulation (GDPR) became applicable in May 2018. Due to the GDPR's extraterritorial scope, which could result in massive fines for U.S. companies, comparative data privacy law is of great current interest. In June 2018, California passed its own Consumer Privacy Act, echoing some of the provisions of the GDPR. Despite the many articles comparing the two schemes of law, little attention has been given to the foundation of these laws, that is, what exactly encompasses the data referred to by these laws? By understanding how the term "personal data" or "personal information" is defined in both jurisdictions, and why these definitions and the treatment of protected data are so different, companies can strategize to take advantage of these developments in the European Union. After explaining the differences in how data is treated in the United States and the European Union by exploring the definitions, regulations, and court cases, we will explore the five legal strategy pathways that companies might pursue with respect to the legal aspects of data transfer and privacy law compliance. While these strategies range from ignoring the law to adopting the European model worldwide, this analysis of legal strategy reveals a means for companies to gain a competitive advantage through their adoption of a worldwide compliance scheme.

*Associate Professor of Business Law, Toulouse Business School.
**Assistant Professor of Legal Studies, Oklahoma State University.
The authors wish to thank Laurie Lucas, Michael Schuster, David Orozco, and the *ABLJ* reviewers for their helpful comments.

INTRODUCTION

On May 25, 2018, the European Union General Data Protection Regulation (GDPR)[1] became applicable, and this proved to be a watershed moment in the area of data privacy.[2] A growing body of academic literature has examined the differences between data privacy laws in the United States and the European Union in relation to the GDPR.[3] Few articles, however, have explained the differences among protected data covered by these laws in a comparative data privacy context.[4] Since legal harmonization seems unlikely at this point due to the current political

[1]Commission Regulation 2016/679, 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 [hereinafter GDPR], 2016 O.J. (L 119) 1 (EU) (repealing Directive 95/46/EC (General Data Protection Regulation) (May 4, 2016)).

[2]*See* Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH. no. 1, (2018), at ¶¶ [53]–[70], https://jolt.richmond.edu/files/2018/11/Houser_Voss-FE.pdf (discussing some of the main changes to EU data privacy law brought by the GDPR, including its extraterritorial scope).

[3]*See, e.g., id.* at ¶¶ [44]–[52] (drawing lessons from a comparison of past U.S. and EU data privacy enforcement actions for enforcement of the GDPR); Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. (forthcoming 2019), https://ssrn.com/abstract=3239930 (arguing that there are "affinities" between U.S. and EU data privacy law and seeing transatlantic data privacy convergence on several points); Paul M. Schwartz, *The EU–U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1974–79 (2013) (commenting on transatlantic divergences after the proposal of the GDPR but before its enactment); Paul M. Schwartz & Karl-Niklaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 119–22 (2017) (taking the angle of "legal identities" on both sides of the Atlantic, in the context of transatlantic data trade); *see generally* Paul J. Watanabe, *An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure*, 90 S. CAL. L. REV. 1111 (2017) (making a comparison of privacy law related to the GDPR's right to erasure).

[4]One exception is a 2014 study by Professors Schwartz and Solove that proposed a new definition of personal information to harmonize the understanding of privacy in the two jurisdictions. Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877 (2014) [hereinafter *Reconciling Personal Information*]. Since the publication date of *Reconciling Personal Information*, a number of factors have made harmonization unlikely such as the Snowden revelations, the Cambridge Analytica data breach scandal, the invalidation of the Safe Harbor, and the enactment of the GDPR. *See infra* Part II.C–D. The same two authors have also categorized elements of the definition of personally identifiable information (PII) in U.S. state data security breach notification laws. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 210–13 (2017).

environment, a new strategy for exploring these differences is necessary.[5] This article details the current differences among definitions of protected data through a comparative study of regulations and case law. This provides the foundation to conduct a legal strategy analysis, based on a framework established by Professors Bird and Orozco that allows firms to rationalize and derive advantage of the two divergent sets of laws and regulations.[6]

The effort taken to disambiguate the differences among definitions of protected data is worthwhile given the importance of the issue and the central role that the definition of "personal data" has in data privacy legislation as the basis for the scope of relevant laws and the development of corporate compliance programs.[7] For example, compliance departments must now map processed data, establish records of personal data processing, and comply with other GDPR requirements. Indeed, the greatest expense of GDPR compliance might involve auditing and classifying data, which hinges on identifying the types of data processed.[8] This in turn will depend on GDPR definitions of personal data and sensitive data, which differ from equivalent U.S. legal definitions.

As an illustration, certain pseudonymized information may be considered de-identified and thus not subject to legislation in the United States.[9]

---

[5]The GDPR became applicable on May 25, 2018. It repealed and replaced the 1995 Directive, which is the legislation the *Reconciling Personal Information* article references. *Reconciling Personal Information*, *supra* note 4 (addressing Council Directive 95/46, 1995 O.J. (L 281) (EC)).

[6]*See infra* Part VI. This framework divides the pathways of legal strategy into stages of increasing legal strategy. The stages are (1) avoidance, (2) compliance, (3) prevention, (4) advantage (or value), and (5) transformation.

[7]As Schwartz and Solove recognized, "'Personal data' is a central concept in privacy regulation around the world. This term defines the scope and boundaries of many privacy statutes and regulations." *Reconciling Personal Information*, *supra* note 4, at 878. *See also* W. Kuan Hon, Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens 10 (2017) (commenting on the concept of "personal data" being critical under EU legislation); Christopher Wolf, *Envisioning Privacy in the World of Big Data*, *in* Privacy in the Modern Age: The Search for Solutions 204, 207–08 (Marc Rotenberg et al. eds., 2015) (commenting on the central nature of personally identifiable information (PII) in information privacy and the lack of uniformity of PII definitions in this area).

[8]*See*, *e.g.*, *The Cost of GDPR Compliance*, HIPAA Journal (May 4, 2018), https://www.hipaajournal.com/the-cost-of-gdpr-compliance/.

[9]*See infra* Part III.F.

Other data, however, similarly treated in the European Union will fail to meet the legal anonymization threshold of personal data that is subject to EU data privacy law protections.[10] Information that might result in identity theft or financial loss may be considered sensitive information subject to additional protections in the United States.[11] The European Union, on the other hand, treats other categories of data that, if disclosed, might result in discrimination (such as political opinions, trade union membership, or past criminal convictions) as sensitive personal data subject to special protections.[12] Companies must, therefore, understand exactly how the information they encounter is subject to various jurisdictions' privacy laws to establish a robust and comprehensive data protection compliance program.[13]

Exactly which information is covered by privacy law? This question becomes increasingly important as the free transfer of data across borders is the key to the profitability and survival of many U.S. companies. Additionally, as pointed out by scholars, the "divergence [of law] is so basic that it threatens the stability of existing policy mechanisms for permitting international data flows."[14] The legal basis for much of the data flow from the European Union to the United States, the Safe Harbor agreement, was invalidated in 2015 and its successor, the EU–U.S. Privacy Shield, remains on shaky ground.[15] Furthermore, the use and definition of terms is

[10]*See infra* Part IV.E.

[11]*See infra* Part III.E.

[12]*See infra* Part IV.D.

[13]*See Reconciling Personal Information*, *supra* note 4, at 879; s*ee also* Phil Lee, *Getting to Know the GDPR, Part 1 —You May Be Processing More Personal Information than You Think*, FIELDFISHER (Oct. 12, 2015 21:12), http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-1-you-may-be-processing-more-personal-information-than-you-think/.

[14]*Reconciling Personal Information*, *supra* note 4, at 877.

[15]Commission Decision 520/2000/EC, 2000 O.J. (L 215) 7 (Aug. 25, 2000) (known as the Safe Harbor). *See* W. Gregory Voss, *The Future of Transatlantic Data Flows: Privacy Shield or Bust?*, J. INTERNET L., May 2016, at 1 (setting out the background of the Safe Harbor, its invalidation, and the development of the Privacy Shield, including the uncertainty that it has engendered from the start); *see also* Kimberly A. Houser & W. Gregory Voss, *The European Commission on the Privacy Shield: All Bark and No Bite?*, U. ILL. J.L. TECH. & POL'Y: TIMELY TECH (Dec. 20, 2018), http://illinoisjltp.com/timelytech/the-european-commission-on-the-privacy-shield-all-bark-and-no-bite/ (discussing the United States's tenuous commitment to the Privacy Shield and risks to the latter). The reasons for the invalidation of the Safe Harbor are discussed briefly *infra* Part II.C.

important in contracts that companies execute related to the export of personal data to the United States, which may be governed by the Privacy Shield's EU definition of personal data.[16]

Comparing personal data as the term is used in the European Union to personally identifiable information as the term is used in the United States is like comparing apples to oranges. Privacy laws in the United States are narrow and sector based, meaning statutes prescribe what information the law covers. For example, a statute may regulate streaming videos, businesses that stream videos, and what the businesses can do with that information. In the Eurpoean Union, data privacy law is much broader and has much wider applicability. All personal data relating to individuals located in the European Union is subject to the GDPR. In this article, we will explain these differences and demonstrate how they may be used strategically by companies to achieve a competitive advantage in the United States and the European Union.

This article is divided into six parts. Following this Introduction, Part I introduces the concept of personal data in the United States and the European Union. Part II provides the bases for privacy protection. Part III describes the categories of personal data and how they are treated under U.S. law. Part IV explains how personal data are defined and treated under EU legislation. Part V explains the importance of the definition of personal data to the GDPR. Part VI sets out the possible pathways for complying with the GDPR and suggests how the differences in the laws may actually provide a strategic advantage for U.S. companies. The following section offers concluding remarks.

---

[16]The EU–U.S. Privacy Shield Framework Principles, which must be respected by self-certifying companies under that scheme, refer to the definition of personal data contained in the 1995 Directive, which was the EU instrument in force at the date of establishment of the Privacy Shield. They provide, "'Personal data' and 'personal information' are data about an identified or identifiable individual that are within the scope of the [1995] Directive, received by an organization in the United States from the European Union, and recorded in any form." U.S. Dep't of Commerce, EU–U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg. The Privacy Shield Framework Principles, with this definition of "personal data," are also contained in Annex II to the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 1, 49 (Aug. 1, 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D1250&from=EN.

I. What Are Personal Data?

The terms "personal information," also referred to as "personally identifiable information" or PII, and "personal data" are central to understanding data privacy law as the terms delimit the scope of the law.[17] In fact, a determination that information is PII may lead to the application of U.S. sectoral privacy statutes and U.S. state data breach notification laws. On the other hand, if information falls within the definition of "personal data" and the material and territorial provisions of the GDPR are met, its legal requirements will apply.

While U.S. statutes use a variety of terms to identify personal data, the most common is PII. We use the term PII to describe the U.S. definition of protected data unless reference is made to a specific statutory definition. The term used in the European Union is "personal data," which was originally defined in Directive 95/46/EC[18] (the 1995 Directive). The term has been interpreted through relevant case law and was slightly modified by the GDPR.[19]

U.S. companies have had difficulty analyzing privacy law in the European Union due to these different concepts regarding what information is subject to protection. The existence of personal data and its processing triggers the application of EU data protection law and any corresponding obligations placed upon data controllers and data processors in light of the rights afforded to data subjects. The GDPR defines "processing" as

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration,

---

[17]*See Reconciling Personal Information*, *supra* note 4, at 888–90. *See also* Ian Kerr & Jessica Earle, *Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy*, 66 Stan L. Rev. Online 65 (2013), https://www.stanfordlawreview.org/online/privacy-and-big-data-prediction-preemption-presumption/ (preferring the "telescope" view of the privacy issue in the context of big data, over the "fine-tuned microscope of data privacy frameworks," to which the definition of PII tends to be a central issue).

[18]Directive 95/46/EC 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 [hereinafter 1995 Directive]; *see infra* Part IV.A.1.

[19]*See infra* Parts IV.B. & IV.A.2.

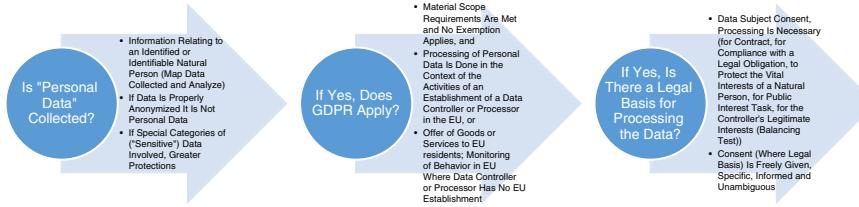

FIGURE 1. The Importance of the Definition of "Personal Data" in the Context of GDPR Compliance. [Color figure can be viewed at wileyonlinelibrary.com]

> retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[20]

The applicability of EU data protection law and its requirements is illustrated in Figure 1. U.S. law, on the other hand, only provides protection for sector-specific PII.

The need to comply with EU law has been underscored by the potential of high administrative fines permitted by the GDPR, which may now amount to billions of dollars.[21] Furthermore, globalization, the growth of electronic commerce, the use of online social networks, cross-border cloud storage, and big data rely on increased transborder data flows.[22] This, together with the extraterritorial effect of EU data protection legislation has made the divergent scope of personal information definitions in relevant legislation an international compliance issue. The next section will explain the bases for privacy protection in the United States and the European Union, and how they fundamentally differ.

II. The Origins of Privacy Protection

In 1980, the Organization for Economic Cooperation and Development (OECD), to which the United States and most of the European Union member states belong, established *Guidelines on the Protection and*

---

[20]GDPR, *supra* note 1, art. 4(2).

[21]*See* Houser & Voss, *supra* note 2, at ¶ [57].

[22]*See* Christopher Kuner, Transborder Data Flows and Data Privacy Law 1–7 (2013).

Transborder Flow of Personal Data.[23] Initially, both jurisdictions incorporated these guidelines into their laws. Although the principles established in these guidelines have remained foundational in European privacy law, including the GDPR, the U.S. privacy regime overall stalled in the 1980s.

It is now widely acknowledged that data privacy law is vastly different in the United States compared to the protections afforded in Europe, particularly in the European Union.[24] The U.S. Department of Commerce stated, "[w]hile the United States and the European Union share the goal of enhancing privacy protection, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation."[25]

These differences color the transatlantic privacy debate and pose problems for companies that operate internationally and wish to comply with these various laws.[26] Privacy is an important concern throughout the

---

[23]OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (revised 2013), https://www.oecd.org/internet/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm [hereinafter OECD Guidelines]; *see* OECD, The OECD Privacy Framework (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf) [hereinafter OECD Privacy Framework].

[24]The United States model has been characterized as a "consumer protection model," as contrasted with the "data protection" model of the European Union "specifically designed from the outset to protect individual privacy or data security." William McGeveran, Privacy and Data Protection Law 257 (2016). Another scholar speaks of a divide between privacy as an aspect of dignity in Western Europe versus privacy as an aspect of liberty in the United States. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 1151, 1161 (2004). *See generally* Schwartz, *supra* note 3.

[25]U.S. Dep't of Commerce, *supra* note 16. Consistent with the description from the Department of Commerce, this distinction has also been described as one between a comprehensive (or omnibus) system in the EU and a self-regulatory/sectoral one in the United States. *See* John Black & Mike Dunne, *Chapter 8: Information Security*, *in* Internet Law for the Business Lawyer 169 (Juliet M. Moringiello ed., 2d ed. 2012).

[26]This is certainly true concerning the European view of the "adequacy" of U.S. data privacy protection related to trans-border data flows between the EU and the U.S. in the context of the negotiation of the EU–U.S. Privacy Shield, mentioned *infra* Part II.C. One study refers to the difference between EU and U.S. data privacy protection as follows: "in the United States, what the European Commission (the EU's executive) refers to as the 'collecting and processing of personal data' is allowed unless it causes harm or is expressly limited by U.S. law. In Europe, by contrast, processing of personal data is prohibited unless there is an explicit legal basis that allows it." Martin A. Weiss & Kristin Archick, *U.S.–EU Data Privacy: From Safe Harbor to Privacy Shield*, CSR Rep. (May 19, 2016) (internal citations omitted).

world, and as a result of cross-border information transfers companies must comply with varying international standards.[27] Not only are the laws different, but the data to which they apply are as well. While an Internet protocol (IP) address may be considered personal data in one jurisdiction and thus protected from disclosure without consent, it may not be considered as such in another jurisdiction.

A. History of U.S. Privacy Law

The U.S. Constitution not only fails to mention data privacy or data protection, it does not mention privacy at all.[28] It was not until 1890, when Warren and Brandeis penned an important article on the right to privacy, and made the argument that the right of privacy is implied by and derived from both the "right to life" and common law and the concept of the right "to be let alone."[29] These rights were expanded to include the right to keep certain personal information out of the public domain.[30]

---

[27]Daniel J. Solove & Paul M. Schwartz, Information Privacy Law 40 (5th ed. 2015) ("Privacy is a global concern. International law and, more precisely, the privacy laws of other countries and international privacy norms, implicate privacy interests in the United States. For example, commercial firms in the United States must comply with the various standards for global commerce…"). One such standard was the 1995 Directive, which was the applicable EU legislation for nearly thirty years until the GDPR became applicable in May 2018. 1995 Directive, *supra* note 18.

[28]As pointed out by one scholar, "[t]he word 'privacy' does not appear in the United States Constitution. Yet concepts of private information and decision making are woven through the entire document, and courts have developed a substantial jurisprudence of constitutional privacy." McGeveran, *supra* note 24, at 3. *See also* Ellen Alderman & Caroline Kennedy, The Right to Privacy xiii (1995). This having been said, another scholar reminds us that "it was a matter of general agreement, in the 1890s, that the Constitution prohibited prosecutors and civil plaintiffs from rummaging through private papers in search of sexual secrets or anything else." Jeffrey Rosen, The Unwanted Gaze 5 (2000). Two commentators speak of "information privacy," contrasting it with "decisional privacy," the latter of which has been at the heart of Supreme Court cases. "Information privacy law is an interrelated web of tort law, federal and state constitutional law, federal and state statutory law, evidentiary privileges, property law, contract law, and criminal law." Solove & Schwartz, *supra* note 27, at 2.

[29]Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 193–95 (1890).

[30]*Id*. at 198.

This idea of the right to privacy has been adopted by the U.S. Supreme Court and throughout the fifty states.[31]

The foundation of the right to privacy is the Fourth Amendment. The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[32] According to one scholar, going beyond the Fourth Amendment, "[w]hat matters in America, over the long run, is liberty against the state within the privacy of one's home."[33]

Although the Fourth Amendment provides no enforcement or privacy protections against private industry's collection and use of personal data, privacy protection does not stop there. Privacy rights have also been recognized against private actors by the courts and in tort law.[34] The Supreme Court has also developed the reasonable expectation of privacy test and the third-party doctrine.[35] One commentator has pinpointed the role of federal legislation in this context: "[w]hen the Fourth Amendment fell short, or Congress didn't like the Supreme Court's interpretation of the Constitution, the federal government enacted laws, generally to protect specific categories of information rather than apply a broader set of privacy principles to all types of data."[36] This resulted in a sector-specific approach toward data privacy law in the United States.

B. EU Data Privacy Law

In contrast to its handling in the United States, data privacy is a fundamental right in Europe. Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), provides, "[e]veryone has the right to the

---

[31]*See* Anne T. McKenna, *Pass Parallel Privacy Standards or Privacy Perishes*, 65 Rutgers L. Rev. 1041, 1046 (2013).

[32]U.S. Const. amend IV.

[33]*See* Whitman, *supra* note 24, at 1214.

[34]*See*, *e.g.*, Department of Commerce Internet Policy Task Force, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (2010) at 10, https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

[35]*See* McKenna, *supra* note 31, at 1046.

[36]*See* Susanna Monseau, Law, Technology, and Business: The 21st Century Corporation and the Future of Work (2017).

protection of personal data concerning them."[37] In addition, article 8(1) of the Charter of Fundamental Rights of the European Union (Charter), provides similarly that "[e]veryone has the right to the protection of personal data concerning him or her."[38] Furthermore, to protect the personal data of those in the European Union, the Charter contains a right to private or family life.[39] According to one commentator, it is generally accepted that fundamental rights are inalienable, and it has been argued that this is based on grounds of human dignity.[40]

This difference in ideology flavors the entire privacy law discussion. In the United States there is an understanding of privacy; however, a company's ability to use information is balanced with an individual's reasonable expectation of privacy. Thus, while U.S. laws cover certain categories of information, such as health information, that one would expect to be kept private, in the European Union there is an overarching protection scheme concerning the personal data of all individuals located within the European Union.

The original definition of "personal data," as discussed in the advisory opinions and court decisions and further elaborated in Part IV originates from the 1995 Directive, which was repealed and replaced by the GDPR on May 25, 2018.[41] The GDPR definition of personal data is quite similar to the 1995 Directive; however, it includes a few additional clarifying examples. All the opinions and cases based on the 1995 Directive and explained below are indicative as to how the GDPR may be interpreted. In other words, if information is not "personal data," the GDPR's protections do not extend to such data.

---

[37]Consolidated Version of the Treaty on the Functioning of the European Union, Oct. 26, 2012, 2012 O.J. (C 326) 47, 55, art. 16(1) [hereinafter TFEU], http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN.

[38]Charter of Fundamental Rights of the European Union, art. 8(1), 2000 O.J. (C 364) 1, 10.

[39]*Id.* art. 7. In addition, it should be noted that the European Convention for Human Rights (which includes among its contracting parties all of the EU member states) also provides a right to respect for private and family life in its article 8. European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, as amended and supplemented. Furthermore, the Council of Europe's Convention 108, which has entered into force in all of the EU member states, seeks to secure data protection. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108, Jan. 28, 1981, https://rm.coe.int/1680078b37.

[40]*See* Orla Lynskey, The Foundations of EU Data Protection Law 241 (2015).

[41]GDPR, *supra* note 1, arts. 99(2) & 94(1). Note that eventually guidance may be issued and court decisions may be rendered on the basis of the GDPR.

C. Cross-Border Transfers

When data was transmitted through the Internet, concerns arose in Europe regarding the differences in privacy expectations among EU member states and among the European Union and other global regimes.[42] The 1995 Directive attempted to harmonize EU member state data protection laws, and cross-border personal data transfer restrictions to third countries outside of the European Union were implemented. Data could not be transferred outside of the European Union unless an adequate level of protection for personal data was offered in the processing country.[43] The United States was not among the countries considered to provide an adequate level of protection. To allow the transfer of data (for example, employee or client data transferred from European subsidiaries to their U.S. parent company), the European Commission and the U.S. Department of Commerce negotiated the "Safe Harbor" agreement.[44]

The Safe Harbor agreement allowed U.S. companies to self-certify their commitment to certain privacy protections. Whether self-certifying U.S. companies knew it or not, the Safe Harbor applied the EU definition of "personal data," referring vaguely to the scope of the 1995 Directive.[45]

---

[42]*See* KUNER, *supra* note 22, at 40 (discussing early EU studies on transborder data flows and EU member state regulation of transborder data flows prior to the adoption of the 1995 Directive). *See also* Barbara C. George et al., *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735, 743–46 (2001) (detailing the EU view of privacy and the impact of the OECD's *Guidelines Governing the Protection of Privacy and Trans-Border Flow of Personal Data* and the Council of Europe's 1981 *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* as the bases for the 1995 Directive, including their support for "restrictions on the transborder transfer of data if the recipient country does not provide a sufficient level of data protection").

[43]Unless a derogation under article 26 of the 1995 Directive applied. 1995 Directive, *supra* note 18, art. 25(1).

[44]*See* Voss, *supra* note 15, at 9.

[45]*See* Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce (2000/520/EC), 2000 O.J. (L 215) 7, 11 ("'Personal data' and 'personal information' are data about an identified or identifiable individual that are within the scope of the [1995] Directive, received by a U.S. organization from the European Union, and recorded in any form."), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0520&from=EN.

After Edward Snowden revealed the espionage conducted by the U.S. government, the Safe Harbor was invalidated by the Court of Justice of the European Union on October 2015.[46] Negotiations between the United States and the European Union ensued shortly thereafter, leading to the replacement of the Safe Harbor by the EU–U.S. Privacy Shield, which became effective on August 1, 2016.[47]

D. Differences in Terminology

The terms PII in the United States and personal data in Europe represent two vastly different concepts. Our analysis aims to investigate privacy regulation's central concept of personal information on both sides of the Atlantic through a comparison of relevant statutes, court cases, and advisory opinions with our focus aimed at the federal (United States) and regional (European Union) levels. This effort is intended to illustrate these differences and their implications for compliance efforts. There is currently no universally accepted data privacy standard or treaty. It is widely acknowledged, however, that EU privacy law has achieved more influence worldwide.[48]

---

[46]*See* Klint Finley, *Thank (Or Blame) Snowden for Europe's Big Privacy Ruling*, WIRED (Oct. 6, 2015, 09:06 PM), https://www.wired.com/2015/10/tech-companies-can-blame-snowden-data-privacy-decision/.

[47]*See* W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 BUS. LAW. 221, 230–32 (discussing the invalidation of the Safe Harbor and the negotiation of the Privacy Shield). The EU–U.S. Privacy Shield was confirmed by the European Commission following its first annual review held in September 2017, with its finding that "the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organisations in the United States," although areas of concern were indicated. *See Report from the Commission to the European Parliament and the Council on the First Annual Review of the Functioning of the EU–U.S. Privacy Shield*, COM(2017) 611 final (Oct. 18, 2017), http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619. Although the Privacy Shield conditionally passed its second-year review, it is possible that due to the continuing surveillance of electronic transmissions by the U.S. government, it could be challenged in the courts. *See* Houser & Voss, *supra* note 15.

[48]*See* MCGEVERAN, *supra* note 24, at 300 ("Most nations outside the US that have adopted significant privacy laws have gravitated toward comprehensive data protection statutes similar to the EU model"); *see also* Schwartz & Peifer, *supra* note 3, at 122 ("EU data protection law has been stunningly influential; most of the rest of the world follows it").

The comparative aspects of data privacy law in the United States and the European Union is of great current interest.[49] This is due to various reasons including the recent application of the GDPR and the attention raised by the negotiation of the EU–U.S. Privacy Shield in 2016.[50] Also, data-related scandals such as the Snowden revelations and the Facebook/Cambridge Analytica scandal have placed data privacy in the international spotlight on both sides of the Atlantic.[51] The next part will explain what data are protected in the United States and the extent of such protection.

III. PII IN THE UNITED STATES

In the United States, privacy law related to individuals' personal information is codified in numerous state and federal statutes. We address the federal statutes before analyzing U.S. court cases and then we look at certain state statutes, including data breach notification laws. Following this, we turn to U.S. views regarding "sensitive data" and de-identification practices.

A. Federal Statutes

Definitions of "personal information" and to whom a related statute applies are sector specific and vary significantly from statute to statute. This is illustrated in the Appendix, where we set out the definitions of "personal information" in relevant federal statutes. It should be emphasized, however, that there is currently no comprehensive data protection law in the United States with respect to Internet privacy.[52] There are,

---

[49]One measure of such interest might be the explosion of web searches in the United States regarding the GDPR since October 2015, just six months before its adoption, as seen using the Google Trends tool, https://trends.google.fr/trends/explore?date=all&geo=US&q=general%20data%20protection%20regulation (last visited on Dec. 29, 2018).

[50]*See* Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU–U.S. Privacy Shield, 2016 O.J. (L 207) 1, Annexes 1 to 7 (Aug. 1, 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D1250&from=EN.

[51]*See, e.g.*, *The Facebook Scandal Could Change Politics as Well as the Internet*, ECONOMIST (Mar. 22, 2018), https://www.economist.com/news/united-states/21739167-even-used-legitimately-it-powerful-intrusive-political-tool-facebook-scandal.

[52]*See* Edward R. Alo, *EU Privacy Protection: A Step Towards Global Privacy*, 22 MICH. ST. INT'L L. REV. 1095, 1110–11 (2013). *See also* Weiss & Archick, *supra* note 26.

however, federal statutes that address specific types of personal information that are subject to privacy protection such as health-care data under the Health Information and Portability Accountability Act (HIPAA),[53] financial data under the Gramm-Leach-Bliley Act (GLBA),[54] children's information under the Children's Online Privacy Protection Act (COPPA),[55] and consumer information under the Fair Credit Reporting Act (FCRA).[56]

In addition, there is no federal legal requirement in the United States for Internet service providers (ISPs) to maintain privacy policies that inform users how their information will be used. Those who do supply privacy policies can be subject to action by the Federal Trade Commission (FTC) for failing to comply with them or otherwise misleading the public.[57] The FTC has taken on the role of "primary regulator of information privacy" in the United States.[58] This has been possible "because it fills the gaps left by the U.S. 'sectoral' regulatory approach."[59] Additionally, there are also several federal statutes that relate more generally to online privacy.[60] These include: the FTC Act,[61] the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act),[62] the

---

[53]Health Information and Portability Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 29 & 42 U.S.C. (2012)).

[54]Gramm-Leach-Bliley Act (Financial Modernization Act of 1999), Pub. L. No. 106-102, 113 Stat. 1338 (codified at 15 U.S.C. §§ 6801-6809 (2012)).

[55]Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277 tit. XIII, 112 Stat. 2681 (codified at 15 U.S.C. §§ 6501–6506 (2012)).

[56]Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1127 (codified at 15 U.S.C. §§ 1681–1681x (2012)).

[57]*See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 600-06 (2014).

[58]Chris Jay Hoofnagle, Federal Trade Commission Privacy Law and Policy xiii (2016).

[59]*Id*. at 145.

[60]For a short description of these, see Marty Solomon, *Bullet Points on a Primer: The Quick Version of the Sedona Conference's Data Privacy Primer*, jdSupra (Jan. 17, 2017), http://www.jdsupra.com/legalnews/bullet-points-on-a-primer-the-quick-79756/.

[61]Federal Trade Commission Act, Pub. L. No. 63-203, 38 Stat. 717, as amended (codified at 15 U.S.C. §§ 41–58 (2012)).

[62]Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified at 15 U.S.C. §§ 7701–7713 (2012)).

Telemarketing and Consumer Fraud and Abuse Prevention Act,[63] the Communications Act of 1934,[64] the Telephone Consumer Protection Act of 1991,[65] and the Video Privacy Protection Act of 1988 (VPPA).[66]

B. U.S. Court Cases

In addition to the very narrow scope of data protected under federal statutes, court cases are also of limited benefit with respect to data privacy because of the conflicting interpretations of these sparse statutes.[67] Due to insufficient precedent, it is difficult for businesses to understand how they must comply with the law.[68] Several court decisions suggest Congress needs to update the laws to reflect current technology.[69] The following are representative court cases that attempt to clarify PII under

---

[63]Telemarketing and Consumer Fraud and Abuse Prevention Act, Pub. L. No. 103-297, 108 Stat. 1545 (codified at 15 U.S.C. §§ 6101–6108 (2012)).

[64]Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (codified at 47 U.S.C. § 151–614 (2012)).

[65]Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (codified at 47 U.S.C. § 227 (2012)).

[66]Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710 (2012), *amended by* Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258, 126 Stat. 2414 (2013)). This statute defines "personally identifiable information" to include "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3). We will review several U.S. federal court decisions involving VPPA *infra* Part III.B.

[67]*See, e.g.*, Transcript of Oral Argument at 44, 130 S. Ct. 2619, http://www.supremecourt.gov/oral_arguments/argument_transcripts/08-1332.pdf. For a recent discussion of this problem, see Jason Tashea, *Courts Need Help When It Comes to Science and Tech*, A.B.A. J. (Nov. 2, 2017, 8:30 AM CDT), http://www.abajournal.com/lawscribbler/article/courts_need_help_when_it_comes_to_science_and_tech/.

[68]*See* City of Ontario v. Quon, 130 S. Ct. 2619, 2630–32 (2010) (adopting a narrow holding that a police department's search of an employee's text messages sent from a cell phone owned and issued by the employer was not unreasonable because it was conducted for a "legitimate work-related purpose"); *see also* United States v. Jones, 132 S. Ct. 945, 949 (2012) (holding that the government violated a criminal suspect's Fourth Amendment rights when it "physically" intruded the suspect's private property).

[69]*See* McKenna, *supra* note 30, at 1050. Although not specific to the definition of PII, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) does demonstrate a nuanced approach to privacy in the United States. In a 5–4 decision, the Supreme Court concluded that the government does need a warrant to obtain location information from a cell phone. This expands the concept of specific information subject to a reasonable expectation of privacy. What is most interesting about this case is the varying viewpoints and rationales in the dissenting opinions. *Id.*

various U.S. statutes. They also demonstrate the difficulty assessing how privacy law should be applied to specific factual scenarios.

In *Spokeo, Inc. v. Robins*,[70] Robins sued Spokeo, a "people search engine," under the FCRA due to the incorrect information it provided about Robins in a consumer report. Because of Spokeo's incorrect report about Robins, the latter alleged that Spokeo had harmed his employment prospects, since such reports could have been provided to potential employers. Robins alleged that Spokeo obtained the information by scraping the Internet without verifying the report's accuracy[71] in violation of the FCRA's requirement that companies use "reasonable procedures to assure maximum possible accuracy" of the report.[72] Although the California district court initially dismissed his claim, the Ninth Circuit reversed indicating that violations of statutes were usually sufficient to show injury.[73] In 2016, the Supreme Court vacated the Ninth Circuit's ruling and remanded the case to make a determination of whether or not Robins had shown that he suffered a "concrete harm."[74] The Supreme Court held that despite language in the FCRA giving individuals a private right of action for violations,[75] this was not sufficient to establish standing.[76] On remand, the lower court found a concrete harm in that the FCRA was intended to prevent dissemination of false information to potential employers and that such false information was likely to impact Robins's job prospects.[77]

Courts have continued to diverge in their interpretations of not only what constitutes personal information, but also whether a violation of federal law intended to protect information is sufficient to establish

---

[70]136 S. Ct. 1540 (2016).

[71]*See* Lauren E. Willis, Spokeo *Misspeaks*, 50 Loy. L.A. L. Rev. 233, 236 (2017).

[72]15 U.S.C. § 1681e(b) (2012).

[73]Robins v. Spokeo, Inc., 742 F.3d 409, 412 (9th Cir. 2014).

[74]*Spokeo*, 136 S. Ct. at 1548.

[75]15 U.S.C. § 1681n (2012).

[76]Justice Ginsburg, joined by Justice Sotomayor, dissented because she felt the complaint sufficiently alleged that the inaccurate report could affect his job opportunities. *Spokeo*, 136 S. Ct. at 1548 (Ginsburg, J., dissenting). A number of scholars also have criticized the holding for this and many other reasons. *See, e.g.*, Willis, *supra* note 71.

[77]Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017).

standing.[78] For example, in *Gubala v. Time Warner Cable, Inc.*, [79] the U.S. Court of Appeals for the Seventh Circuit affirmed the lower court's decision that consumers do not have standing to sue companies for violating the Cable Communications Policy Act (CCPA) without proof of harm.[80] The CCPA requires cable operators to destroy consumers' PII if the "information is no longer necessary for the purpose for which it was collected."[81] Gubala argued that although he canceled his Time Warner Cable (TWC) account in 2006, TWC had retained his personal information, including his name, address, Social Security number, phone numbers, and credit card information in violation of the CCPA.[82] Since the unlawful retention of the information could subject the company to a data breach or transfer to an unknown entity, it was necessary for the company to delete the information that was no longer relevant to its business operations as required by statute.[83] The court concluded that the risk of harm was not sufficient to establish standing.[84] This seems contrary to *Spokeo*—cited in *Gubala*—since that case ultimately found on remand a risk of harm to the individual due to a potential misuse of PII.

Comparable divergence can be found in what constitutes PII under the VPPA. Similar to the CCPA, the VPPA provides a private right of action for violations of the statute. In *Yershov v. Gannett Satellite Information Network, Inc.*, the court held that under the VPPA, PII includes the GPS coordinates of a device.[85] Yershov argued that Gannett's *USA Today* Mobile App violated the VPPA by sharing with external parties: (1) the title of the video viewed, (2) the GPS coordinates of the device at the time

---

[78]*See* Brief of Nat'l Ass'n of Prof. Background Screeners as Amicus Curiae in Support of Petitioner, at 6–7, Spokeo v. Robins, 136 S. Ct. 1540 (2012), https://www.supremecourt.gov/DocketPDF/17/17-806/26868/20180105135803107_17-806%20Spoker%20Inc.%20v.%20Robins_A-1b.pdf.

[79]846 F.3d 909 (7th Cir. 2017).

[80]Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779.

[81]47 U.S.C. § 551(e) (2012); CCPA defines "personally identifiable information" in the negative: "the term 'personally identifiable information' does not include any aggregate data which does not identify particular persons." 47 U.S.C. § 551(a)(2)(A).

[82]*Gubala*, 846 F.3d at 911.

[83]*Id.*

[84]*Id.*

[85]No. 15-1719 (1st Cir. Apr. 29, 2016).

the video was viewed, and (3) unique device identifiers.[86] Because external parties could combine this information with information from other sources, they were able personally to identify Yershov and the videos he was watching.

On January 9, 2017, the Supreme Court denied certiorari to *In re Nickelodeon Consumer Privacy Litigation*,[87] allowing the U.S. Court of Appeals for the Third Circuit's 2016 decision to stand holding that IP addresses were not PII and not subject to the VPPA's privacy protections.[88] The circuit court of appeals had stated that digital identifiers, such as media access control (MAC) addresses and IP addresses, were not PII because the VPPA's definition of PII "applies only to the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior."[89] The opinion acknowledged the ruling in *Yershov*, but distinguished *Nickelodeon* by saying that a global positioning system (GPS) location is more likely to identify a specific person than an IP address.[90]

---

[86]Christin McMeley & John D. Seiver, *1st Circuit and FTC Address Definitions of "PII," While Michigan Amends Privacy Law to Remove Statutory Damages*, Davis Wright Tremaine LLP (May 11, 2016), http://www.dwt.com/First-Circuit-and-FTC-Address-Definitions-of-PII-While-Michigan-Amends-Privacy-Law-to-Remove-Statutory-Damages-05-11-2016/.

[87]C. A. F. v. Viacom Inc., 137 S. Ct. 624, 196 L. Ed. 2d 516 (2017).

[88]*In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262 (3d Cir. 2016). *See* Ani Gevorkian, *U.S. Supreme Court Denies Cert in Video Privacy Protection Act Case*, Nat'l L. Rev. (Jan. 10, 2017), https://www.natlawreview.com/article/us-supreme-court-denies-cert-video-privacy-protection-act-case (describing the effect of the denial of certiorari on the Third Circuit's decision).

[89]*Nickelodeon*, 827 F.3d at 267. For a discussion of this case, see Ani Gervorkian, *U.S. Supreme Court Denies Cert In VPPA Case*, Covington Inside Privacy (Jan. 10, 2017), https://www.insideprivacy.com/united-states/litigation/u-s-supreme-court-denies-cert-in-vppa-case/.

[90]*See Nickelodeon*, 827 F.3d at 289 ("GPS coordinates contain more power to identify a specific person than, in our view, an IP address, a device identifier, or a browser fingerprint."). For a further discussion of this case, see Christin McMeley et al., *Definition of "PII" Under VPPA Continues to Evolve with 3rd Circuit Ruling*, Privacy and Sec'y L. Blog (July 7, 2016), http://www.privsecblog.com/2016/07/articles/comms-media/definition-of-pii-under-vppa-continues-to-evolve-with-3rd-circuit-ruling/. *Cf.* Frederik Zuiderveen Borgesius, *The* Breyer *Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition*, 3 Eur. Data Prot. L. Rev. 130 (2017) (wherein the author explains European law, which indicates that users can be readily identified from IP addresses in certain situations).

As these cases illustrate, U.S. courts are loath to explain the limits or expand the definition of PII and seldom rule in favor of consumers, holding that there must be some recognizable harm.[91] In other words, it seems that despite clear violations of U.S. privacy statutes, unless a plaintiff's identity was stolen due to the complained of violation, a plaintiff is seldom deemed to have standing under these federal statutes.[92] This is contrary to the European Union's handling of these situations where the failure to comply with the law (such as wrongful disclosure) could result in an enforcement action against the company that caused the disclosure, even without a showing of harm.[93] In addition, unlike in *Gubala*, where the U.S. court held that failure to delete data was not a harm, the GDPR permits enforcement actions and fines against a company that fails to delete data upon request from a data

[91]The majority of cases regarding data breaches are pursued under state law (data breach statutes). For a detailed list of such state data breach notification laws see SOLOVE & SCHWARTZ, *supra* note 4, at 205–13.

[92]*See generally* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737 (2018). For example, after Wyndham Hotels experienced three data breaches in a two-year period, the FTC brought an action against them for failing to secure their customer's data as promised in their privacy policy. The Third Circuit Court of Appeals affirmed the lower court's action, ruling in the FTC's favor. In this case, the data breach caused more than $10.6 million in fraud loss. In 2015, Wyndham settled the FTC charges and agreed to perform annual audits of its security practice for twenty years and to notify the FTC of any future breaches within ten days. Press Release, FTC, Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment. In *FTC v. LabMD*, the court held that the FTC's order requiring the company to enact "reasonable security measures" was too vague and as such unenforceable. The court noted that the FTC has the authority to require companies to implement specific security measures but had not done so in this case. LabMD v. FTC, No. 16-16270 (11th Cir. 2018). It should be noted that the main difference in *Wyndham* and *LabMD* is that there was actual harm to consumers in the *Wyndham* case. Because the actions of the companies complained of was so similar, and the results so different, these types of actions do not provide consistent guidance to businesses using consumer data.

[93]Bart van der Sloot, *Where* is *the Harm in a Privacy Violation? Calculating the Damages Afforded in Privacy Cases by the European Court of Human Rights*, 8 JIPITEC 322 (2017), https://www.jipitec.eu/issues/jipitec-8-4-2017/4641/JIPITEC_8_4_2017_322_van_der_Sloot.

subject. Under European law both GPS coordinates[94] and IP addresses[95] may be considered personal data.

C. U.S. State Statutes and the California Consumer Privacy Act of 2018

While every state has some type of privacy law or data breach notification law,[96] they also each have their own definition of PII.[97] California has the most inclusive statutes, and they are the most comparable to EU laws.

Referred to as the mini-GDPR by some,[98] the California Consumer Privacy Act (CaCPA)[99] is the most comprehensive statute in the United States regarding data privacy law. After anticipated changes, this new law will go into effect January 2020 and will apply to any business that meets one of the following thresholds: (1) annual gross revenues of $25 million; (2) obtains personal information of 50,000 or more California residents, households, or devices annually; or (3) fifty percent or more annual revenue from selling California residents' personal information.[100]

The motivation behind the law is similar to the GDPR and is to provide statutory protection and remedies for all California residents. It defines "personal information" as "any information that … relates to … a particular consumer or household."[101] The term "personal information" is defined broadly and includes unique identifiers, geolocation data, and inferences from consumer behavior.[102] It gives consumers a right to

---

[94]The GDPR now explicitly includes location data in the definition of personal data. *See* GDPR, *supra* note 1, art. 4(1).

[95]*See*, *e.g.*, Case C-70/10 Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (Nov. 24, 2011), [2011] ECR I-12006, ¶¶ 15–20 [hereinafter Scarlett v. SABAM], http://curia.europa.eu/juris/celex.jsf?celex=62010CJ0070&lang1=fr&type=TXT&ancre=.

[96]Data breach notification statutes are discussed *infra* Part III.D.

[97]For a breakdown of these state statutes, see Solove & Schwartz, *supra* note 4, at 210.

[98]*See*, *e.g.*, *California Enacts Mini-GDPR Effective January 1, 2020*, jdSupra (Jan. 5 2018), https://www.jdsupra.com/legalnews/california-enacts-mini-gdpr-effective-74873/.

[99]California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.198(a) (2018).

[100]Cal. Civ. Code § 1798.140(c)(1).

[101]*Id.* Several exceptions apply to this definition, such as for "publicly available information" (Cal. Civ. Code §1798.140(o)(2)) and "commercial conduct [that] takes place wholly outside of California" (Cal. Civ. Code §1798.145(a)(6)).

[102]Cal. Civ. Code §1798.140(o)(1).

know how their information is being used, the right to delete, and the right to stop businesses from selling their personal information.[103]

While some feel the CaCPA is a harbinger of things to come,[104] the senior legislative counsel at the American Civil Liberties Union believes that the tech industry's recent push for a federal privacy statute is because it preempts more stringent state law.[105] According to the Electronic Frontier Foundation, the tech industry does not want to be personally liable to consumers in the event of a data breach as the CaCPA would require.[106] They would prefer to have the FTC enforce a watered-down federal privacy statute.[107] Interestingly, it is the states that have led the way in consumer privacy protections with their data breach notification laws.[108]

---

[103] (i) Therefore, it is the intent of the Legislature to further Californians' right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights:

(1) The right of Californians to know what personal information is being collected about them.
(2) The right of Californians to know whether their personal information is sold or disclosed and to whom.
(3) The right of Californians to say no to the sale of personal information.
(4) The right of Californians to access their personal information.
(5) The right of Californians to equal service and price, even if they exercise their privacy rights.

CAL. BUS. & PROF. CODE § 22577(a) (2016). Assembly Bill No. 375, § 2. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375.

[104] For a discussion of certain updates to state privacy laws, made either shortly before or after the application date of the GDPR, see Jeewon Kim Serrato et al., *US States Pass Data Protection Laws on the Heels of the GDPR*, DATA PROT. REP. (July 9, 2018), https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/.

[105] *See* Neema Singh Guliana, *The Tech Industry Is Suddenly Pushing for Federal Privacy Legislation. Watch Out.*, WASH. POST (Oct. 3, 2018), https://www.washingtonpost.com/opinions/the-tech-industry-is-suddenly-pushing-for-federal-privacy-legislation-watch-out/2018/10/03/19bc473e-c685-11e8-9158-09630a6d8725_story.html?utm_term=.dbb810463b2d.

[106] Dina Temple-Raston, *Why the Tech Industry Wants Federal Control over Data Privacy Laws*, NPR (Oct. 8, 2018), https://www.npr.org/2018/10/08/654893289/why-the-tech-industry-wants-federal-control-over-data-privacy-laws.

[107] *Id.*

[108] California was the first U.S. state to enact a data breach notification statute and require companies collecting personal data to conspicuously display a privacy policy. CAL. CIV. CODE § 1798.82(a) (West 2018); *see also* California Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE § 22577(a) (West 2018).

D. U.S. State Data Breach Notification Laws

Certain U.S. states have data breach laws that are of interest, since they provide definitions of personal information that, if breached, triggers the requirements under the relevant statute.[109] Solove and Schwartz have studied PII definitions in state data breach notification laws and have found divergence among such definitions. There is some convergence, however, in that all forty-seven states studied by them and the District of Columbia consider Social Security numbers, driver's license numbers or state identification card numbers, and financial account numbers, such as a credit card number, as elements of PII. By contrast, three states provide that a name is not necessary as an element for PII to exist, four states include medical information, five states include biometric data, and only one state includes telecommunication access devices and DNA profiles.[110] One corporate counsel summarizes the coverage of personal information in these statutes as follows:

> Most state laws define personal information as a combination of pieces of information that discloses the identity of someone. For example, in Nevada, personal information is defined as a natural person's first name or first initial and last name in combination with one or more other data elements that include: Social Security number, driver's license number, credit card number, health insurance identification number, electronic mail address with password. Under California's statute, the definition of personal information is much broader …. Most state laws exclude from the definition of personal information any information that is publicly available by legal means.[111]

It is clear from the foregoing that a core subset of information is largely accepted as personal information, and that a minority of states include certain other elements as personal information in their statutes.

---

[109]HIPAA and GLBA also have data breach notification requirements.

[110]Solove & Schwartz, *supra* note 4, at 210–11. All remaining states have since adopted data breach notification laws, bringing the total to fifty states. *See* Daniel Solove, *Breach Notification Laws Now in All 50 States*, TeachPrivacy (Apr. 7, 2018), https://teachprivacy.com/breach-notification-laws-now-in-all-50-states/ (the last two states to adopt laws were South Dakota and Alabama).

[111]*See* Catherine Bragg, *Data Breach Notification: State Law Requirements*, 18(2) Under Construction (Winter 2017), https://www.americanbar.org/publications/under_construction/2017/winter2017/data_breach_notification_state_law_requirements.html.

E. A U.S. View of "Sensitive Data"

There is no explicit U.S. legislative category of "sensitive data," in contrast to EU data protection law. As indicated by Solove and Schwartz,

> Such a category [sensitive data] does not exist as a general matter in U.S. privacy law. Yet, U.S. law does extend heightened protection to certain data through specific laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA). But, for the most part, U.S. law does not globally recognize types of data that receive heightened protection across various laws akin to EU-style "sensitive data."[112]

In addition to the data afforded heightened protection under HIPAA, as mentioned by Solove and Schwartz, data that if "hacked" could lead to identity theft or financial loss, could be considered "sensitive data" in the United States as indicated by the following statement by the FTC in the context of the Equifax data breach: "[i]f you have a credit report, there's a good chance that you're one of the 143 million American consumers whose *sensitive* personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies."[113] In that case, data that was hacked included people's names, Social Security numbers, birth dates, addresses and driver's license numbers, credit card numbers, as well as dispute documents.[114]

A Pew Research Center report on cybersecurity cites account numbers as an example of sensitive information, and indicates that financial and health information are likewise sensitive.[115] Furthermore, Nancy J. King and V.T. Raja argue that children's personal information collected by websites should be included in that classification along with personal information collected by financial institutions, personal health information, and

---

[112]*Reconciling Personal Information*, *supra* note 4, at 906.

[113]Seena Gressin, *The Equifax Data Breach: What to Do*, Federal Trade Comm'n Consumer Info. (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do (emphasis added) (the author is an attorney in the Division of Consumer & Business Education at the FTC).

[114]*Id.*

[115]Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, Pew Res. Ctr. Internet & Tech. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/. "35% [of Americans] have received notices that some type of sensitive information (like an account number) had been compromised." The report on the same study later states, "But some of these [online] services compel users to submit highly personal or sensitive information, such as details of users' financial records or medical history." *Id.*

credit histories,[116] while admitting that "there is no clear starting point for defining sensitive data in the United States" analogous to that in the European Union, "largely because there is no similar generally applicable data protection regulation in the United States."[117]

Our discussion of EU data protection law, on the other hand, will demonstrate that the concept of "sensitive data" is set forth explicitly in the law, as are the consequences for the collection and treatment of such data.[118]

F. De-Identification of Data Under U.S. Law

Certain information that would otherwise be subject to privacy protection in the United States may no longer be subject to such protections if it is "de-identified."[119] Under HIPAA, for example, once health information is de-identified, there are no longer restrictions on its use or disclosure. This is contained in the related section 164.514(a) of the HIPAA Privacy Rule, as amended: "(a) Standard: De-identification of protected health information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information."[120] "De-identified" in this context means that the health information no longer identifies "nor provides a reasonable basis to identify" an individual, and this may occur in one of two ways: either there may be a "formal determination by a qualified statistician" or "the removal of specified identifiers of the individual and of the individual's relatives, household members, and employees" where the "covered entity has no actual knowledge that the remaining information could be used to identify the individual."[121]

Potentially, de-identification may involve "pseudonymization," which is defined by the National Institute of Standards and Technology as a "particular type of anonymization that both removes the association

---

[116]*See* Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 Am. Bus. L.J. 413, 424–25 (2013).

[117]*Id*. at 424 (citation omitted).

[118]*See infra* Part IV.D.

[119]*See Reconciling Personal Information*, *supra* note 4, at 907–08.

[120]45 C.F.R. § 164.514(a) (2011).

[121]*See* McGeveran, *supra* note 24, at 762.

with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms."[122] De-identification may be used under HIPAA,[123] and potentially this could involve pseudonymization together with safeguards and controls for certain data sets:

> When organizations overlay [pseudonymous data] with safeguards and controls, the data move further down the identifiability spectrum to *Protected Pseudonymous* data. Limited data sets under the HIPAA are an example of data in this category. They comprise Protected Health Information (PHI) that excludes direct identifiers and various categories of indirect identifiers, but explicitly includes other indirect identifiers that must be scrubbed under the HIPAA de-identification Safe Harbor standard … They may be used or disclosed subject to strict use agreements, for purposes of research, public health, or health care operations.[124]

Under the FTC's three-part test,[125] pseudonymous data "could in certain circumstances be considered de-identified," although the "legal rules around pseudonymous data are equally inconsistent."[126]

G. Summary of U.S. Data Privacy Law

As is clear from the foregoing, the focus in the United States on PII definitions has less to do with the collection and processing of such data and more to do with security requirements and data breach notification issues. There is no general federal data privacy legislation in the private sector, and the sectoral laws that exist are of limited scope and based on the kind of data covered or the persons protected. Uniformity is lacking, and much of the data that are covered under privacy law in the European Union fall through this legislative gap.

---

[122]Simson L. Garfinkel, *De-Identification of Personal Information*, NISTIR 8053, Oct. 2015, at 2, http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf (citation omitted).

[123]*See* Chris Achatz & Susan Hubbard, *US vs. EU Guidelines for De-Identification, Anonymization and Pseudonymization*, J. Internet L., May 2017, at 1, 8.

[124]Jules Polonetsky et al., *Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification*, 56 Santa Clara L. Rev. 593, 615 (2016).

[125]Federal Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change 21 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[126]*Id.*

If we look at the state level, there is a wide array of statutes in different states with widely varying PII definitions. However, as in the case of the federal statutes, the definitions are built with lists of specific elements of data that are covered. All fifty states now have data breach notification laws with lists of data that are covered by the statutory requirements. While these vary greatly, all forty-seven state laws studied by Solove and Schwartz have a core of basic information that is covered: Social Security numbers, driver's license numbers or state identification card numbers, financial account numbers, and credit card numbers.[127]

While there is no overarching legislative category of "sensitive data," data, which if hacked would lead to identity theft, and children's data and health data could be considered "sensitive." The pseudonymization of data may sometimes result in information treated as "de-identified" and thus no longer subject to certain requirements of law.

IV. Personal Data in the European Union

The treatment and scope of personal data in the European Union is essentially different than that of PII in the United States. While in the United States the statutes apply to specific categories of information, with restrictions on the use of those categories of information, and with the restrictions only applying to the designated industries or agencies that handle that information, the European Union utilizes one general definition for protected data—personal data. The definition is meant to be a broad one aimed at protecting individuals' right to privacy. In our investigation of personal data, we first detail the definitions of personal data in EU legislation. We develop these definitions further through EU court decisions, organized into categories of personal data. Next, we deal with data breach notification and sensitive data under EU law. This is followed by a discussion of data de-identification and a summary of EU law.

A. EU Legislation

In this section we detail the definition of personal data in EU legislation both before and after May 25, 2018. This is important, not only to give a historical perspective, but to allow comparison of the definitions and

[127] *See supra* Part III.D.

the inclusion in later law of court cases expanding the definition of personal data.

1. The 1995 Data Protection Directive

Personal data, as defined in the 1995 Directive, means

> [A]ny information related to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[128]

First, the initial words of this text nearly mirror those of the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which date back to 1980: "'personal data' means any information relating to an identified or identifiable individual (data subject)."[129] The same definition was supplied in the Council of Europe's Convention 108, which was signed the following year and ratified by the EU member states, among other contracting parties.[130]

Second, this definition focuses on the ability of one to identify a data subject. Specifically, identification numbers are listed, but so are other factors, when they relate to other elements of a person's identity. Recital (26) of the 1995 Directive specifies that "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person" and that "data rendered anonymous in such a way that the data subject is no longer identifiable" are no longer subject to the protection provisions of the 1995 Directive.[131]

2. GDPR

The definition of personal data in the GDPR is almost identical to that in the 1995 Directive:

---

[128]1995 Directive, *supra* note 18, art. 2(a).

[129]OECD Guidelines, *supra* note 23, para. 1(b). These Guidelines were revised in 2013 but the definition of "personal data" remained unchanged. *See* OECD Privacy Framework, *supra* note 23, para. 1(b). It is worth noting that the United States is a member of OECD. http://www.oecd.org/about/membersandpartners/.

[130]Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, C.E.T.S. No. 108, art. 2(a), https://rm.coe.int/1680078b37.

[131]1995 Directive, *supra* note 18, recital (26).

> [A]ny information relating to an identified or identifiable natural person ("data subject"); 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.[132]

This new definition expands on the concept by adding genetic identity to the other factors to which the data may refer. These additions take into consideration developments of new technologies and practices such as use of DNA analysis, and incorporation of GPS and other location data into smartphone applications.

B. EU Court Cases

In contrast to U.S. case law, the court cases of EU member states are more instructive in reference to the definition of personal data. Also, the courts of the European Union "ensure that in the interpretation and application of the Treaties the law is observed."[133] The nomenclature of the EU courts changed after the adoption of the Treaty of Lisbon, and the Court of Justice of the European Union includes the Court of Justice (ECJ), the General Court (formerly known as the Court of First Instance), and specialized courts.[134] The ECJ is the highest court within the Court of Justice of the European Union and "[t]he [ECJ]'s interpretation of EU law, such as the [1995 Directive], are binding on member states."[135] The areas of jurisdiction of the Court of Justice of the European Union (and thus the ECJ) include, inter alia, enforcement actions, review of legality, review of inaction, and preliminary rulings.[136]

Member state national courts may raise preliminary questions to the ECJ on the interpretation of treaties and the validity and interpretation of acts of EU institutions and bodies, for example, where the national court "considers that a decision on the question is necessary to enable it to give judgment."[137] The result is a preliminary ruling, which is the form taken by the judgments handled in this section.

---

[132]GDPR, *supra* note 1, art. 4(1).

[133]Paul Craig, The Lisbon Treaty: Law, Politics, and Treaty Reform 122–23 (2010).

[134]*Id.* at 122–23.

[135]McGeveran, *supra* note 24, at 281–82.

[136]Craig, *supra* note 133, at 124.

[137]TFEU, *supra* note 37, art. 267.

EU court cases illustrate the very wide scope of the definition of personal data, which includes names and addresses,[138] names used in conjunction with a telephone number,[139] biometric data,[140] and video images of individuals.[141] To illustrate the differences between U.S. and EU handling of, respectively, PII and personal data, we have chosen to detail three EU cases, each dealing with a distinct form of personal data.

1. Health Information

Unlike HIPAA, under EU data privacy law there is no requirement regarding who holds health information for it to be considered personal data, as is illustrated by the following case. The *Bodil Lindqvist* case[142] involved data that included information about the health of covolunteers at a Swedish church. The data were held by an individual, Mrs. Lindqvist, and published

---

[138]Case C-553/07, College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, 2009 ECR I-03889, ECLI:EU:C:2009:293, ¶ 42 (May 7, 2009), http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=74028&occ=first&dir=&cid=981919 (involving a reference to a preliminary ruling from a Dutch court that relates to the partial refusal of the Board of Aldermen of Rotterdam (the College) to grant Mr. Rijkeboer access to information on the disclosure of his data to third parties during the two-year period prior to his request).

[139]Case C-101/01, Bodil Lindqvist, 2003 ECR I-12971, ¶¶ 2, 13–14, (Nov. 6, 2003), http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=30128 (involving a request for a preliminary ruling made by a court in Sweden, where criminal proceedings were brought before the court against Mrs. Lindqvist for breach of Swedish data protection legislation for publishing on her personal web site information on co-volunteers at a Swedish church, sometimes including their full names (or just first names), jobs held, hobbies, family circumstances, telephone numbers, and in one case information about a physical injury and medical leave, without their consent).

[140]Case C-291/12, Michael Schwarz v. Stadt Bochum, 2013 ECR I-12971,ECLI:EU:C:2013:670, ¶¶ 1–2 (Oct. 17, 2013), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0291 (involving a request for a preliminary ruling from a German court concerning the City of Bochum's refusal to issue Mr. Michael Schwarz a passport unless his fingerprints—a form of biometric data—were collected at the same time to be stored in the passport).

[141]Case C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů [Office for Personal Data Protection] 2015 O.J. (C46/6), ECLI:EU:C:2014:2428, ¶¶ 1–2 (Dec. 11, 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62013CJ0212 (involving a request for a preliminary ruling from a court of the Czech Republic in which the Czech Office for Personal Data Protection found that Mr. Ryneš had committed various data protection violations in connection with the installation of a camera system located under the eaves of his family home, allowing a visual recording stored on a hard disk drive).

[142]*See Bodil Lindqvist*, *supra* note 139.

on her personal website. The court found that the information about a physical injury to the foot and about a medical leave constituted "data concerning health," which falls within the special categories of personal data. As the court stated, "[r]eference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46."[143]

This relatively early case, while defining various information as "personal data," may not seem to us today to add anything surprising in this regard. Nonetheless, Solove and Schwartz refer to this as a "Sweeping Decision": "[The ECJ] read the [1995 Directive]'s provisions about personal data about health to extend even to a mention of a foot injury. Without the data subject's permission, such personal information could not be subject to processing."[144] Another commentator discussed this case in these terms: "[s]o, although we might think that there is a considerable difference between disclosing a named individual's medical record online and simply naming a person online, for the ECJ both acts of data processing engage the data protection regime (albeit that different provisions are made for justifying the acts in question)."[145]

2. Working Time Information

The difference between U.S. and EU treatment of personal information in a work setting is particularly striking. In the European Union, data protection law applies to employers, and consent standards for data processing are high because of the inherent power employers have over employees. In the United States there are no general or sectoral laws governing the protection of the personal information of employees.[146]

---

[143] *Id.* ¶ 51.

[144] Solove & Schwartz, *supra* note 27, at 1147.

[145] Roger Brownsword & Morag Goodwin, Law and the Technologies of the Twenty-First Century: Text and Materials 309–10 (2012).

[146] In the EU, comprehensive data protection law covers employers in the same fashion as other data processors, and regulators tend to be particularly strict in cases involving workplace information. For example, most European regulators apply consent standards especially rigorously in employment-related cases, requiring very explicit affirmative agreement or even finding valid consent unobtainable because of what they view as the inherent power differential in the employment relationship . . . . In the US, however, there is no single law, not even a sectoral statute, that governs the privacy of employee data across the board.

McGeveran, *supra* note 24, at 665.

One example of the EU treatment is a case involving working time information.

The legal action underlying *Worten v. ACT* involved the Portuguese Authority for Working Conditions (ACT)'s request for access to Worten's record of working time.[147] The question was, is the "personal data" definition of the 1995 Directive to be interpreted to include "the record of working time, that is, the indication in relation to each worker, of the times when working hours begin and end, as well as the corresponding breaks and intervals"?[148]

The ECJ (Third Chamber) found that it did.[149] By this decision, one can see the ties to the individual inherent in much information, allowing it to meet the criteria of the concept of "information relating to an identified or identifiable natural person."

3. IP Addresses

Breyer v. Federal Republic of Germany is a relatively recent case involving a reference for a preliminary ruling from a German court regarding the Federal Republic of Germany's registration and storage of the IP address assigned to Mr. Breyer when accessing websites of German Federal institutions.[150]

The ECJ (Second Chamber) distinguished *Breyer* from *Scarlet v. SABAM*.[151] The latter concerned the collection and identification of IP addresses of Internet users by ISPs, whereas in Breyer it is the online media provider,

---

[147]This case involves a request for a preliminary ruling from a Portuguese court on, inter alia, 1995 Directive, *supra* note 18, art. 2. Case C-342/12, Worten—Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT), 2013 O.J. (C225/37), ECLI:EU:C:2013:355, ¶¶ 1–2 (May 30, 2013), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0342.

[148]*Id.* ¶ 7.

[149]"The data contained in a record of working time such as that at issue in the main proceedings, which concern, in relation to each worker, the daily work periods and rest periods, constitute personal data within the meaning of Article 2(a) of Directive 95/46, because they represent 'information relating to an identified or identifiable natural person.'" *Id.* ¶ 19 (citations omitted).

[150]Case C-582/14, Patrick Breyer v. Bundesrepublik Deustchland, ECLI:EU:C:2016:779, ¶¶ 1–2 (Oct. 19, 2016) [hereinafter Patrick Breyer], http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0582&lang1=fr&type=TXT&ancre=.

[151]*See* Scarlet v. SABAM, *supra* note 95.

in this case the Federal Republic of Germany, that registers IP addresses of users, albeit without the means to directly identify the users.[152]

Furthermore, the court noted that dynamic IP addresses were involved—"provisional addresses which are assigned for each internet connection and replaced when subsequent connections are made."[153] According to the ECJ in this case, a dynamic IP address "does not constitute information relating to an 'identified natural person', since such an address does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer."[154]

The phrase "information relating to an 'identified natural person'" refers to one element of the definition of "personal data" in the 1995 Directive, the other being information relating to an identifiable natural person, that is, a person "who can be identified, directly or indirectly"; therefore the information alone does not have to identify the person.[155] Account should be taken of "all the means likely reasonably to be used either by the controller or by any other person to identify" that person.[156] Information that enables identification does not have to be held by the same person.[157] Here, the ECJ found that the media provider had means for identification with the help of the competent authority and the ISP.[158] That would not have been the case, however, if the identification obtained from the IP address and data held by the ISP was either prohibited by law or "practicably impossible" because it required "a disproportionate effort in terms of time, cost and man-power."[159] As a result, in this case the ECJ found that the definition of "personal data" in the 1995 Directive must be interpreted to include

---

[152]*See* Patrick Breyer, *supra* note 150, ¶¶ 33–35.

[153]*Id.* ¶ 36.

[154]*Id.* ¶ 38.

[155]*Id.* ¶¶ 40–41.

[156]*Id.* ¶ 42.

[157]*Id.* ¶ 43.

[158]*Id.* ¶ 48.

[159]*Id.* ¶¶ 45–46.

> [A] dynamic IP address registered by an online media service provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to the provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.[160]

Thus, IP addresses in the hands of a media provider are considered personal data under certain conditions, in addition to those IP addresses in the hands of an ISP, as discussed in *Scarlet v. SABAM*.

The cases in this part applied the definition of personal data under the 1995 Directive,[161] which has been incorporated (as modified) into the definition of personal data under the GDPR.[162] This suggests the desire to harmonize data privacy law among the EU member states.[163] It also stands in contrast to the piecemeal approach in the United States where different courts interpret the same law differently, as is glaringly evident in the case of U.S. courts' inconsistent treatment of IP addresses.[164]

C. Data Breach Notification

In the European Union, data breach notification was not incorporated generally into EU data protection law until the GDPR. Article 33 reads as follows:

> In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.[165]

This very short time frame varies significantly from U.S. state data breach notification requirements, which range from as soon as possible to sixty days after discovery.

---

[160] *Id.* ¶ 49.

[161] *See supra* Part IV.A.1.

[162] *See supra* Part IV.A.2.

[163] *See infra* Part IV.F.

[164] *See supra* Part III.B.

[165] GDPR, *supra* note 1, art. 33.

D. Sensitive Data in the European Union

The GDPR sets out a category of sensitive information known as "special categories of information," which includes "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[166] These categories of data are subject to additional protections and restrictions on processing. The general rule is that their processing is prohibited.[167] A list of exceptions, however, applies such as when the data subject has given "explicit consent," so long as no applicable member state law prevents the lifting of the prohibition;[168] or when the processing is necessary in the context of carrying out obligations or exercising rights related to employment and is authorized by law;[169] or where the data is manifestly made public by the data subject.[170]

E. De-Identification of Data

The European Union makes a distinction between anonymized data and pseudonymized data. In another opinion, the Article 29 Working Party (WP29) underscored that "[o]nce a dataset is truly anonymised and individuals are no longer identifiable, European data protection law no longer applies."[171] In other words, the relevant data are no longer considered "personal." WP29 warned that for this to be true, the data must be made anonymous "in such a way that the data subject is no longer identifiable."[172] That is, the anonymization must be "irreversible."[173] WP29 has

---

[166]*Id.* art. 9.

[167]*Id.*

[168]*Id.* art. 8(2)(a).

[169]*Id.* art. 8(2)(b).

[170]*Id.* art. 8(2)(e).

[171]Working Party, *Opinion 05/2014 on Anonymisation Techniques* (Apr. 10, 2014) (WP 216) [hereinafter WP 216], at 5, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[172]1995 Directive, *supra* note 18, recital (26).

[173]WP 216, *supra* note 171, at 5.

provided guidance as to the main points that data controllers should consider with respect to anonymization techniques and their robustness, focusing on the "guarantee attainable by the given technique taking into account the current state of technology and considering three risks which are essential to anonymization:" singling out, linkability, and inference.[174]

The position of WP29 has been described as "requiring near-zero probability, an impractical standard."[175] Furthermore, WP29 reminds us that

> Pseudonymisation is also addressed to clarify some pitfalls and misconceptions: pseudonymisation is not a method of anonymisation. It merely reduces the linkability of a dataset with the original identity of a data subject, and is accordingly a useful security measure. In order for data to be taken out of the definition of personal data it [sic] has to be properly anonymized; pseudonymization is not enough.[176]

Moreover, Recital (26) to the GDPR makes it clear that personal data that have been pseudonymized remain personal data; however, a different conclusion is reached for anonymized data that would take considerable time and money to reidentify:

> [t]o ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. 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 longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.[177]

---

[174]*Id.* at 11–12.

[175]Polonetsky et al., *supra* note 124, at 604 (citation omitted). As two authors state, WP29 does, in its opinion, "include statements that it is sympathetic to a risk-based approach," acknowledging the difficulty in creating a "truly anonymous dataset," as combining two such data sets may lead to identification. Sophie Stalla-Bourdillon & Alison Knight, *Anonymous Data v. Personal Data—A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, 34 Wis. Int'l L.J. 284, 297 (2017) (Stalla-Bourdillon & Knight's article includes a discussion of the UK DPA's opinion on anonymization, not covered by this study).

[176]WP 216, *supra* note 171, at 3.

[177]*See* GDPR, *supra* note 1, recital (28).

In the case of an effective anonymization, the relevant individual is no longer an identified or identifiable person to whom the information (data) are related; thus, the data fall out of the definition. However, three scholars highlight that the European Commission's staff has noted that anonymization and pseudonymization have been a "major area of divergent interpretation" among EU member states, especially regarding pseudonymized data under certain conditions.[178]

F. Summary of EU Data Privacy

EU data privacy or data protection law is based on the existence of what is defined in relevant statutes as "personal data," and their processing. As has been shown, these definitions are largely harmonized and made uniform through a system of cross-references between statutes, and by the application of the GDPR, which as a regulation will be directly applicable in the same form throughout the European Union.[179] Nonetheless, prior to such date, some differences exist in the way member state legislation implemented the definition of "personal data" from the 1995 Directive. Moreover, the definition of "personal data" is broad and open-ended, allowing for its wide interpretation by courts in favor of the individual and the maintenance of his or her fundamental rights. Furthermore, it is the processing of such data that results in rights and obligations, and infringement of the law may lead to an administrative fine imposed by an independent EU member state supervisory authority, commonly referred to as a data protection agency (DPA), without any need to establish proof of financial harm.[180]

Thus, we have seen that personal data may exist in many contexts: personal, professional, and even where data are already public: there is no requirement that the data be private. The broad definition allows for

---

[178]*See* Polonetsky et al., *supra* note 124, at 602.

[179]Article 288 of the TFEU sets out the differences between directives and regulations as follows:

> A regulation shall have general application. It shall be binding in its entirety and directly applicable in all member states. A directive shall be binding, as to the result to be achieved, upon each member state to which it is addressed but shall leave to the national authorities the choice of form and methods.

TFEU, *supra* note 37, art. 288, at 171–72.

[180]*See* GDPR, *supra* note 1, art. 83(1)–(2). For a short discussion of administrative fines, see *supra* Part VI.B.

the inclusion of data used by future technologies and new methods of doing business. Again, the data subject does not have to be identified by the data but merely identifiable by them. One French practitioner lists certain examples of elements that can identify a person and that therefore fall within the definition of personal data. These examples help illustrate that definition's wide scope under the GDPR and include the following: name, photo, fingerprint, biometric data, physical, physiological, genetic, psychic, economic, cultural or social identity, unique style of dress, telephone location data, license plate number, embossed credit card number, online identifier (opening of an account), e-mail address, IP address, cookies, online behavioral data,[181] and avatars,[182] among others.

V. GDPR Compliance

U.S. firms may be subject to elements of EU compliance law because they conduct business in the European Union, receive personal data through the Privacy Shield, are subject to the increased extraterritorial application of the GDPR in connection with the offering of goods or services to EU residents, or because they monitor individual behavior that occurs in the European Union. As detailed in Figure 1, the first step to achieve compliance in the European Union is to determine whether "personal data" are present, then whether the GDPR applies, and lastly whether there are legal bases for processing the data. The first part involves mapping the data collected by the company.

As discussed above, EU law is different from U.S. law by its omnibus nature, scope (as illustrated by its broad and open-ended definition of "personal data"), and its underlying basis. Depending on the applicable jurisdiction, the definition of what is considered personal information may vary. One study refers to this difference between EU data protection law and a privacy law system as it exists in the United States as follows: "[EU] Data protection law uses objective definitions for personal data and sensitive personal data, unlike [U.S.] privacy law's subjective

[181] Règlement européen sur la protection des données: Texte, commentaires et orientations pratiques [European General Data Protection Regulation: Text of the Law, Comments, and Practical Guidance] 19 (Alain Bensoussan ed., 2016) [Fr.].

[182] *Id.* Here the author cites a personalized avatar such as the one used in Pokemon Go®.

'reasonable expectations.' This results … in a binary, all or nothing perspective, and wide-ranging applicability."[183]

Unless a U.S. company is part of the industry targeted by a sector-specific statute, for example, a bank dealing in financial information or a hospital dealing in health information, there are few legal restrictions on a company's use of data. In other words, exchanging data for services is not only legal, but encouraged to allow these companies to innovate.[184] While state laws do affect companies' dealings, these laws are fairly limited in scope.[185] As we have previously argued, the main challenge is an FTC enforcement action for "unfair and deceptive practices" such as failing to comply with a privacy policy that the company itself created.[186]

Furthermore, there is a lack of international harmonization when it comes to data privacy law. The authors of one essay believe it is unlikely that a global data privacy regulation regime will develop.[187] The 1995 Directive and now the GDPR, however, have considerable influence internationally and have eclipsed the U.S. sectoral privacy law approach.[188]

Prior to conducting a legal strategy analysis, the requirements of the GDPR with respect to personal data will be explained. Due to the extra-territorial application of this regulation, businesses dealing with personal data from the European Union will need to adapt their compliance programs to meet these requirements.

---

[183]W. Kuan Hon et al., *The Problem of "Personal Data" in Cloud Computing: What Information Is Regulated?—The Cloud of Unknowing*, 1(4) Int'l Data Privacy L. 211, 213 (2011).

[184]FTC, FTC's Privacy Report: Balancing Privacy and Innovation (2012), https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report.

[185]With the exception of the CaCPA becoming effective January 2020. CaCPA, *supra* note 99.

[186]*See* Houser & Voss, *supra* note 2, at ¶ [14].

[187]Jürgen Feick & Raymund Werle, *Regulation of Cyberspace, in* The Oxford Handbook of Regulation 523, 536 (Robert Baldwin et al., eds., 2010).

[188]*See*, *e.g.*, Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. Times (May 24, 2018), https://nyti.ms/2Lq0rAC (commenting on the likelihood of nations like Brazil, South Korea, and Japan following the European Union's lead on data protection legislation). Regarding Asia, see Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives 12 (2014) (describing first the influence of OECD Guidelines, and since the mid-1990s, the equally important impact of the 1995 Directive on Asian data privacy laws).

A. A Lawful Basis for Data Processing

Once it is established that personal data are present and that the GDPR applies, a lawful basis for processing that data under the GDPR must be established.[189] A lawful basis may be that the data subject has given his or her consent to processing for specific purposes.[190] This is the legal basis that most often comes to mind.[191] However, it is not the only basis. For example, processing may be "necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract."[192] Furthermore, there is a legal basis for processing when necessary "for the purposes of the legitimate interests pursued by the controller," subject to a balancing of interests with fundamental rights of the data subject, particularly when he or she is a child.[193]

B. Recordkeeping of Activities Related to Data Processing

The GDPR institutes an obligation of accountability on data controllers. This involves being able to prove compliance at any given time. For

---

[189]The GDPR defines "processing" as

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

GDPR, *supra* note 1, art. 4(2).

[190]*Id.* art. 6(1)(a). That consent is subject to certain conditions having been met. *See id.* art. 7. It also must be a "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." *Id.* art. 4(11).

[191]*See, e.g.*, Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies 63 (2018) (calling "consent" the "linchpin" of the GDPR, legitimizing "most kinds of data collection, use and disclosure") (citation omitted).

[192]GDPR, *supra* note 1, art. 6(1)(b). However, one commentator indicates that the term "necessary" in this context is strictly construed, which might limit the usefulness of this basis. *See* Lynskey, *supra* note 40, at 31–32.

[193]GDPR, *supra* note 1, art. 6(1)(f). This basis may continue to give rise to problems of interpretation under the GDPR. *See, e.g.*, Lynskey, *supra* note 40, at 33. In the case of sensitive data, the potential bases for processing are more restrictive. *See* GDPR, *supra* note 1, art. 9(2).

example, if the legal basis for processing mentioned earlier is the consent of the data subject, the controller must be able to "demonstrate that the data subject has consented to processing of his or her personal data."[194] An important new requirement is that data controllers and processors keep detailed records of processing activities, which must be made available to the supervisory authority upon request.[195] This obligation does not apply to small- and medium-sized enterprises with fewer than 250 employees, unless the processing involves sensitive data, data relating to criminal convictions and offenses, or unless it "is likely to result in a risk to the rights and freedoms of data subjects" or is "not occasional."[196]

C. *The Requirement to Hire a Data Protection Officer*

The GDPR establishes the requirement that certain firms designate a data protection officer or DPO.[197] This individual is seen as an intermediary between the company and the member state's DPA and is tasked with the responsibility for "the implementation and supervision of internal processes to ensure compliance with the GDPR."[198] The DPO should not receive instructions regarding the carrying out of his or her tasks, should not be dismissed for carrying out his or her tasks, and should report to the highest management level within the company.[199]

In companies that are required to designate a DPO under the GDPR, such DPO may help differentiate between "general" personal data and "sensitive" personal data, as these categories will involve different requirements:

---

[194]GDPR, *supra* note 1, art. 7(1).

[195]*Id*. art. 30(1)–(4).

[196]*Id*. art. 30(5).

[197]*Id*. art. 37(1). This requirement applies when public authorities or bodies carry out processing, or when "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 where core activities consist in the "processing on a large scale" of sensitive data or data about criminal convictions and offenses. *Id*. art. 37(1)(a)–(c).

[198]Nicolò Ghibellini, *Some Aspects of the EU's New Framework for Personal Data Privacy Protection*, 73 Bus. Law 207, 207 (2017).

[199]GDPR, *supra* note 1, art. 38(3).

> It is important for DPOs and organizations to distinguish, in advance of collecting personal data, whether the proposed data collection relates to general personal data or sensitive personal data. They also need to be able to confirm compliance procedures in advance of collecting and maintaining personal data, particularly sensitive personal data.[200]

A DPO or equivalent corporate officer in companies not required to have a DPO should perform an audit to understand what data his or her organization holds and the purpose of such data usage.[201] Practically speaking, it would be the DPO's job to decide if personal data is being processed by his or her employer and to document such processing.

D. Data Subject Rights

The GDPR provides data subjects with certain rights that already existed under the 1995 Directive, for example, the right to access the personal data being processed,[202] the right to rectify inaccurate data,[203] the right to restrict data processing under certain circumstances,[204] the right to object to processing personal data,[205] the right not to be subject to a decision that produces legal effects based solely on automated processing including profiling,[206] and the requirement of transparency.[207] Furthermore, the GDPR provides new data subject rights such as the right to erasure also known as the "right to be forgotten"[208] and the right to data portability.[209] Compliance efforts must now provide adequate means to receive requests regarding the exercise of these rights and the appropriate oversight of efforts taken to comply with these laws and regulations.

---

[200]Paul Lambert, The Data Protection Officer 36 (2017).

[201]*Id.* at 221.

[202]GDPR, *supra* note 1, art. 15.

[203]*Id.* art. 16.

[204]*Id.* art. 18.

[205]*Id.* art. 21.

[206]*Id.* art. 22.

[207]*Id.* arts. 12–14.

[208]*Id.* art. 17.

[209]*Id.* art. 20.

VI. Compliance Pathways

The GDPR has generated strong reactions among companies who process data internationally. Much of the discussion has been negative, with parties claiming the new law will impose significant costs for compliance without a meaningful return.[210] Research on law and strategy, however, gives us a lens to examine the shift in view regarding what personal data means and how firms can respond to the GDPR in an efficient manner.[211] As legal scholar Constance Bagley explains, law can be used not only to control risk but to create value for a business if used strategically.[212]

To illustrate this in the context of GDPR compliance, which utilizes the broadest definition of personal data, we use Bird's pathways of legal strategy framework.[213] Bird's theoretical framework provides an excellent way for companies to conceptualize the GDPR compliance issue, since the framework sets out the analysis in five different stages. Later extensions of the framework by Bird and Orozco also included a similar five-stage process, based on five legal strategies or pathways, though this later work restates the fourth step as "value" rather than "advantage."[214] Our analysis refers to both the original and the later discussions, but maintains Bird's original terminology. The comparative analysis of U.S. and EU law undertaken here is applied to each stage in the framework and helps highlight the varying efficiencies and benefits that companies might

---

[210]*See* Jeremy Kahn et al., *It'll Cost Billions for Companies to Comply with Europe's New Data Law*, Bloomberg Businessweek (Mar. 22, 2018), https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law.

[211]*See* Michael E. Porter, *What Is Strategy?*, Harv. Bus. Rev. (Nov–Dec. 1996), at 61, 62–64, https://hbr.org/1996/11/what-is-strategy; Robert C. Bird, *Pathways of Legal Strategy*, 14 Stan. J.L. Bus. & Fin. 1, 1 (2008); George J. Siedel, Using the Law for Competitive Advantage 136 (2002).

[212]Constance E. Bagley, *Winning Legally: Using the Law to Create Value, Marshal Resources, and Manage Risk*, Case No. 9-806-138 (Harvard Business School ed., Aug. 4, 2006); *see generally* Constance E. Bagley, *Winning Legally: The Value of Legal Astuteness*, 33 Acad. Mgmt. Rev. 378 (2008); Constance E. Bagley, *What's Law Got to Do With It?: Integrating Law and Strategy*, 47 Am. Bus. L.J. 587 (2010).

[213]*See* Bird, *supra* note 211, at 12–26.

[214]*See* Robert C. Bird & David Orozco, *Finding the Right Corporate Legal Strategy*, 56 MIT Sloan Mgmt. Rev. 81, 82 (2014), https://sloanreview.mit.edu/article/finding-the-right-corporate-legal-strategy/ (positing a scale of five pathways of corporate legal strategy: Avoidance (being the lowest level), Compliance, Prevention, Value, and Transformation).

obtain in each of these stages. Bird and Orozco indicate that companies might achieve the greatest impact at stage five of their framework. We see strategic advantages at each stage of compliance, but in this context, we assert that the transformation that occurs at stage five could provide the greatest benefits. Companies that adopt the protections afforded by the GDPR and the CaCPA, not only in the United States and Europe, but worldwide, should realize the greatest competitive advantage.

A. Stage One: Avoidance

Bird and Orozco note that although some companies may consider the law as an obstacle to their business goals, an "avoidance strategy can sometimes be effective."[215] When confronted with changes in the regulatory environment, companies simply choose to ignore them, or engage in what Bird calls "avoidance."[216] This is the lowest level option for the company. In this context, the strategy is to avoid the implications of the changes in EU law by the U.S. firm, that is, until the law becomes a problem. For example, prior to the GDPR, a firm without a physical establishment in the European Union might have sought to simply avoid EU law by carrying out data processing activities outside of the European Union (say, in the United States). However, to do so legally would require the use of the Safe Harbor or its successor, the Privacy Shield, or some other legal basis for the cross-border transfer of such data.[217] Using such a strategy might result in short-term success, since there is evidence of a lack of FTC enforcement of the Safe Harbor, so the chances of being prosecuted might be slim.[218]

Some firms also might respond by simply blocking access to their websites in the European Union. This strategy has been adopted by a number of American news outlets such as the *Los Angeles Times*, the *New York Daily News*, and the *Chicago Tribune*.[219] If you were to click on

---

[215]*See id.*

[216]*See* Bird, *supra* note 211, at 12.

[217]*See supra* Introduction.

[218]According to Chris Jay Hoofnagle, the FTC's first substantive enforcement action under the Safe Harbor was the Google "Buzz" matter. This occurred in 2011—ten years after the Safe Harbor was adopted. *See* Hoofnagle, *supra* note 58, at 323.

[219]Rebecca Hill, *US Websites Block Netizens in Europe: Why Are They Ghosting EU? It's Not You, It's GDPR*, The Register (May 25, 2018), https://www.theregister.co.uk/2018/05/25/tronc_chicago_tribune_la_times_gdpr_lock_out_eu_users/.

the *Los Angeles Times* website, for example, while in Europe, you would see this message:

> Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.[220]

Although an avoidance strategy may work for smaller firms that do not rely on a European audience for customers or expansion, it will not eliminate issues for businesses, including news outlets, with a European customer base. As Professors Bird and Orozco put it, "An avoidance strategy can sometimes be effective—a company might, for example, want to outsource certain activities to another jurisdiction to avoid burdensome local regulations—but it can also lead to disasters."[221] As we will argue, compliance with the GDPR now offers companies a better, long-term strategic option.

B. Stage Two: Compliance

The next pathway is the compliance level.[222] Similar to avoidance, a compliance strategy views legal adherence as a cost of doing business.[223] However, rather than avoiding the law, this strategy involves compliance at a minimum level.[224] Although one might have put Facebook in the avoidance category prior to the GDPR, given the several DPA actions brought against it, it is more accurately categorized as pursuing the compliance pathway.[225] In this category, the law is seen as "an unwelcome

---

[220]Adam Satariano, *U.S. News Outlets Block European Readers over New Privacy Rules*, N.Y. Times (May 25, 2018), https://www.nytimes.com/2018/05/25/business/media/europe-privacy-gdpr-us.html. More than 1000 U.S. news sites were still unavailable in the European Union as of August 7, 2018. Jeff South, *More Than 1,000 U.S. News Sites Are Still Unavailable in Europe, Two Months After GDPR Took Effect*, Nieman Lab (Aug. 7, 2018), http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.

[221]*See* Bird & Orozco, *supra* note 214, at 82.

[222]Bird, *supra* note 211, at 16–22.

[223]*See id*. at 16.

[224]*See id*. at 19.

[225]Certain of these actions are detailed in Houser & Voss, *supra* note 2, at ¶¶ [30]–[35] (discussing the Facebook Safe Harbor and cookies cases).

but mandatory constraint" on a company's activities.[226] As Bird and Orozco put it, "[s]trategic opportunities do not exist unless executives make a deliberate decision to engage in noncompliance activities after taking into account the consequences and costs of doing so. Indeed, some managers might appreciate the legal duties imposed on their business but choose noncompliance after a careful cost-benefit analysis."[227]

At the compliance level, companies should understand the differences between the personal data and personal information definitions and apply the broader EU personal data standard correctly when it is applicable. A firm could perhaps reason that under the 1995 Directive, sanctions for data protection violations were relatively low prior to the application of the GDPR, and DPAs might not result in maximum administrative fines.[228] Fines could then be seen as the cost of doing business, and firms could choose noncompliance after weighing the financial risk. However, things have changed since the GDPR increased sanctions, some of which may amount to more than a billion euros for larger tech companies [229] or up to four percent of worldwide turnover for the most serious violations.[230] Also, DPAs may now order the temporary or definitive halting of data processing, therefore the dynamics have certainly changed.[231] This is true as a result of the increased extraterritorial reach of the GDPR.

Considering the case of Facebook, apparently that company is not about to adopt Bird's Stage Three pathway. Facebook has limited the coverage of its Irish subsidiary, which used to be the Facebook entity

---

[226]Bird & Orozco, *supra* note 214, at 83.

[227]*Id.* at 84.

[228]The UK DPA, the UK Information Commissioner's Office (ICO), was given authority to impose fines of up to £500,000 but only imposed a total of £2 million in fines in 2015. *See* Simon Davies, *The Data Protection Regulation: A Triumph of Pragmatism over Principle?*, 2 Eur. Data Prot. L. Rev. 290, 292 (2016) (citing the ICO's Annual report for 2015/2016).

[229]For Facebook, the maximum amount of a potential fine has been calculated as equivalent to $1.6 billion. Adam Satariano, *New Privacy Rules Could Make This Woman One of Tech's Most Important Regulators*, N.Y. Times (May 16, 2018), https://nyti.ms/2GjRTaN. Nonetheless, as the article points out, one limitation is faced by Ireland's DPA: the data protection commissioner has a low budget, and a small staff with which to regulate Internet giants, such as Facebook, which has "hundreds of people globally working on data protection regulation alone, including lawyers and privacy experts hired in Dublin." *Id.*

[230]GDPR, *supra* note 1, art. 83(5).

[231]*Id.* art. 58(2)(f).

contracting with users outside of North America, to residents of the European Union. As pointed out by others, "[t]hat means non-EU users will no longer be able to appeal to European data protection authorities to uphold EU rules …"[232] It is reported that Facebook clarified its CEO Mark Zuckerberg's statements to Congress, by saying the he "only outlined that the new privacy controls under GDPR, and not the other regulatory requirements, would be applied to Facebook's global network."[233] As Professor Wu, a former senior adviser at the FTC, put it, "Facebook's DNA is unchangeable: their basic idea is to amass as much data as possible, and press the limits on sharing it."[234]

C. Stage Three: Prevention

Although compliance and prevention involve assessing current legal risks, prevention involves creating a legal strategy to avoid future legal problems down the road.[235] At this stage, a business would adopt forward-thinking procedures to not only avoid enforcement actions, but to anticipate what European DPAs might be looking for and address those issues in advance. This could include Privacy Impact Assessments and the remediation of any problems discovered as opposed to waiting for an audit by a DPA. This is how a true legal strategy begins: by anticipating issues and working in advance to handle them.

For example, the Seattle-based mobile payments start-up Remitly began mapping out their entire inventory of user data, updating privacy policies, and building tools to let customers access their personal information, delete it, and move it to other services, all prior to the date the GDPR became applicable.[236] The General Counsel pointed out that while U.S. tech companies

---

[232]Mark Scott & Nancy Scola, *Facebook Won't Extend EU Privacy Rights Globally, No Matter What Zuckerberg Says*, Politico (Apr. 21, 2018), https://www.politico.eu/article/facebook-europe-privacy-data-protection-mark-zuckerberg-gdpr-general-data-protection-regulation-eu-european-union/.

[233]*Id.* (Zuckerberg had previously told U.S. lawmakers that Facebook would extend the GDPR to users worldwide).

[234]Seth Fiegerman, *Facebook Faces New Regulatory Backlash over Data Privacy*, CNN (June 4, 2018), http://money.cnn.com/2018/06/04/technology/facebook-data-backlash/index.html.

[235]Bird, *supra* note 211, at 22.

[236]Monica Nickelsburg, *Race to the GDPR Finish Line: How US Tech Companies Are Preparing for Europe's Stringent New Privacy Law*, GeekWire (May 24, 2018), https://www.geekwire.com/2018/race-gdpr-finish-line-us-tech-companies-preparing-europes-stringent-new-privacy-law/.

are in a much worse position due to the light regulations they had been operating under, Remitly had already been complying with the privacy regulations relating to financial data and, as such, had a shorter way to go.[237]

Although Facebook and Google claimed to have complied with the GDPR,[238] enforcement actions were brought against them immediately upon the applicable date of the GDPR.[239] In contrast, Amazon Web Services (AWS) explained on May 26, 2018, what it had already accomplished in anticipation of the GDPR. They had conducted a service readiness audit to examine whether they had the technical and organizational measures in place to secure the personal data that they held, obtained International Organization for Standardization or ISO certifications in a number of areas (none of which are required by the GDPR but demonstrate a forward-thinking procedure), published a white paper on how its current product and service offerings will assist their customers with compliance,[240] and although not specifically required, detailed how they had gained compliance with the Cloud Infrastructure Service Providers in Europe Code of Conduct prior to the GDPR's applicable date.[241]

D. Stage Four: Advantage

Similar to the prevention stage, the advantage stage involves using compliance with the law as a business strategy.[242] This option goes beyond integrating a legal practice with beneficial nonlegal activities by reframing

---

[237]*Id.*

[238]Scott & Scola, *supra* note 232.

[239]*See, e.g.*, Chris Foxx, *Google and Facebook Accused of Breaking GDPR Laws*, BBC (May 25, 2018), https://www.bbc.com/news/technology-44252327.

[240]Amazon Web Services, Inc., Navigating GDPR Compliance on AWS (Nov. 2017), https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf.

[241]Chad Woolf, *All AWS Services GDPR ready*, AWS Security Blog (Mar. 26, 2018), https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/.

[242]Bird, *supra* note 211, at 26. This section should be read while keeping in mind that certain voices have been raised claiming that "incumbents," such as Facebook and Google, may benefit from the GDPR. *See, e.g.*, Daisuke Wakabayashi & Adam Satariano, *How Facebook and Google Could Benefit from the G.D.P.R., Europe's New Privacy Law*, N.Y. Times (Apr. 23, 2018), https://nyti.ms/2HpH9Nl (The authors state that firms such as Google and Facebook "still have an advantage because advertisers are likely to turn to service with reach and enormous audience." However, the authors also report that tech giants would be "under a microscope," according to European Data Protection Supervisor Giovanni Buttarelli.).

the legal problem as an opportunity.[243] Take Microsoft's announcement that it would provide the same data subject rights required under the GDPR to its customers worldwide.[244] Although not explicit in the announcement, by using the broader EU definition of "personal data" worldwide to determine the data it chose to protect, Microsoft could avoid having to create different policies based on where its users are located, creating great efficiencies in the handling of privacy and data security issues. By applying GDPR rights to customers worldwide, Microsoft can streamline and generalize the processes for handling data subjects' rights discussed in Part V.D. Instead of a multitude of laws, Microsoft would be subjecting itself primarily to one, the GDPR. By doing so, Microsoft could potentially achieve value through efficiencies and lowered compliance costs.[245] Compliance costs could be further reduced and redundancies eliminated by combining the roles of the required DPO with their current Chief Privacy Officer (CPO) and make the position responsible for data protection law compliance worldwide.[246]

---

[243]Bird, *supra* note 211, at 25–30.

[244]Julie Brill, *Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data*, Microsoft on the Issues (May 21, 2018), https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/.

[245]In a parallel, when the European Commission first proposed the GDPR, its then Justice Commissioner Viviane Reding put forth the savings to companies of having one set of rules instead of twenty-seven or twenty-eight (one for each EU member state) as an argument for the proposal. "A single set of rules on data protection, valid across the EU. Unnecessary administrative requirements, such as notification requirements for companies, will be removed. This will save businesses around €2.3 billion a year." *See* European Commission Press Release IP/12/46, *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses* (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm.

[246]However, the roles are not entirely the same. While the DPO is to report to the highest levels in the organization, his or her role is to ensure compliance. The practice in U.S. firms is that the CPO takes more of a strategic forward-planning role, so companies would need to change their expectations if they were to adopt a DPO for activities worldwide in the place of a CPO. Professors Bamberger and Mulligan describe the results of their research on U.S. practices as follows:

> The CPOs described a forward-looking focus on identifying future challenges rather than compliance with existing mandates. They also underscore the potential for environmental ambiguity, combined with credible threats of meaningful sanction, to affect the scope of the privacy function within corporate organizations. Our respondents described a broad reach throughout the corporation, authority to participate in strategic decisions about the firm business, and relatively wide latitude to establish corporate practices and define their jobs.

Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Ground: Driving Corporate Behavior in the United States and Europe 194–95 (2015).

If a company were to choose the same option as Microsoft did, it could also avoid having to verify for each jurisdiction what is included in the definition of "personal information" or "personal data." As we have seen, the GDPR's definition of personal data covers all of the elements included in PII or personal information. Furthermore, the adoption of the EU definition would fit with the requirements of the Privacy Shield and other mechanisms for cross-border transfer of data. In fact, the Privacy Shield's predecessor, the Safe Harbor, has been credited with having caused some companies "to extend Continental-style protections to American consumers."[247]

Moreover, by complying with the spirit of EU data protection laws, companies may be able to minimize the likelihood of new data protection class-action lawsuits in the European Union.[248] Likewise, aggressive compliance efforts may be taken into account by supervisory authorities when they determine the amount of administrative fines when a violation does occur.

Finally, by complying with the GDPR, U.S. firms would be preparing themselves for compliance worldwide.[249] Through annexes to trade agreements, and because there is no viable alternative coming from the United States, the European model of data protection is gaining traction worldwide. Currently this is notable in Asia as well as in Latin America. It is reported that "Brazil, Japan and South Korea are set to follow Europe's lead," with some having already passed similar laws, and that "European officials are encouraging copycats by tying data protection to some trade

---

[247] *See* Hoofnagle, *supra* note 58, at 328.

[248] The possibility of these lawsuits by civil liberties or consumer protection representatives is provided for in GDPR article 80. Injunctions may be issued to order a halt to data processing. *See* Julia Powles, *The G.D.P.R., Europe's New Privacy Law, and the Future of the Global Data Economy*, New Yorker (May 25, 2018), https://www.newyorker.com/tech/elements/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-data-economy.

[249] In fact, similar to this argument, but somewhat different, is that those companies that are subject today to constraints because they comply with existing U.S. sectoral privacy laws may find that this allows them more easily (and with less incremental cost) to comply with the GDPR. However, firms in sectors where there is no existing U.S. sectoral legislation may suffer the highest incremental costs associated with GDPR compliance. This logic is consistent with what is happening internationally. For European companies, GDPR compliance costs have been found to be less than what U.S. companies spend, generally, because "many of the requirements of GDPR already exist in EU law and companies have advanced systems in place to deal with them." *See* Oliver Smith, *The GDPR Racket: Who's Making Money from This $9bn Business Shakedown*, Forbes (May 2, 2018), https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#3116c5c634a2.

deals and arguing that a unified global approach is the only way to crimp Silicon Valley's power."[250] European Justice Commissioner Věra Jourová recently visited Tokyo where she worked on negotiating data protection adequacy arrangements there. She highlighted what she argued was the value of the GDPR and strong data protection law when she said,

> GDPR offers important benefits for businesses both European and foreign. For instance, the harmonisation and simplification brought about by the GDPR will make life much easier for companies, as they will now only have to deal with one set of rules. They will also benefit from reduced compliance costs and flexible tools to meet their obligations.[251]

E. Stage Five: Transformation

Closely related to the advantage stage, the transformation stage leverages these advantages in a way that can potentially change the businesses' mission.[252] Given the Cambridge Analytica debacle, U.S. tech companies have lost a great deal of credibility. Combined with the applicability of the GDPR, consumers are becoming more aware of the loss of privacy and potential security issues involved with many U.S. tech companies. No longer are consumers as willing to provide their data in return for free services. In fact, Facebook's social media market share has declined from a high of eighty-two percent in July 2017 to approximately sixty-nine percent in November 2018.[253] Indeed, the protection of privacy has a value for consumers, and according to one technology journalist, citing examples

---

[250]Satariano, *supra* note 188.

[251]Speech of Commissioner Jourová at the Public Event Dedicated to the GDPR and International Data Transfers in Tokyo: New EU Privacy Law as an Opportunity to Boost Both Trade and Data Protection Standards (May 31, 2018).

[252]Bird, *supra* note 211, at 30. Although Bird's article speaks about the transformation stage as providing a competitive advantage that is retainable over the long term, we diverge slightly by focusing on the characteristic of creating value when none exists. In the Bird & Orozco article, the authors indicate that the transformative stage is difficult to replicate by competitors. Bird & Orozco, *supra* note 214. As any company could adopt this advanced strategy of a worldwide compliance program which anticipates where the law is heading as evidenced by both the European model being highly influential and California having influence throughout the United States, we vary from this part of the definition in focusing on the potential cost savings and efficiencies (as well as the trust gained) by companies who adopt a single method for handling data collected from any location in the world.

[253]*Social Media Stats Worldwide—August 2018*, STATCOUNTER, http://gs.statcounter.com/social-media-stats (last visited on Dec. 29, 2018).

of what might be described as privacy by design and default,[254] Apple's best product today and "the single biggest reason that consumers should choose an Apple device over competing devices—is privacy."[255]

Data protection is directly linked to trust since individuals who are afraid that others will not respect their privacy, or fail to protect the security of their data, quickly lose confidence and will be reluctant to share their data. Trust is therefore a key resource of the digital economy.[256] The trust that Commissioner Jourová spoke about is potentially another reason for companies to take the action that Microsoft took. It was announced on July 17, 2018, that Japan and the European Union had reached agreement on the adequacy of each other's data protection, and that a formal adequacy decision was expected by the European Union in autumn 2018.[257] U.S. tech companies can leverage their compliance with the GDPR to change and improve their corporate culture, resulting in greater trust among consumers. By going above and beyond the legal requirements, such as AWS did in the last example, and advertising such measures to the public, they can gain a distinct trust-based competitive advantage over firms who minimally comply with the law.

Forward-thinking companies who adopt this fifth path will get ahead of potential U.S. regulation as well. The CaCPA will go into effect January 1, 2020. California is often a bellwether for legislation

---

[254]In a similar vein, data protection by design and default is a requirement of the GDPR. GDPR, *supra* note 1, art. 25.

[255]Michael Grothaus, *Forget the New iPhones: Apple's Best Product Is Now Privacy*, FastCompany (Sept. 13, 2018), https://www.fastcompany.com/90236195/forget-the-new-iphones-apples-best-product-is-now-privacy (The author also indicates that Apple may have an advantage over Facebook and Google in the sense that its business model is not built on monetizing personal data; however, that does not take anything away from his claim that "Apple seems to be the only major tech company that had the foresight—and the will—to begin tackling these issues before they reached a crisis point."). It may be argued that companies in certain U.S. sectors may benefit from varying expectations of consumers, as a 2015 Pew Research Center survey indicated regarding confidence that records would remain private and secure. *See* Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Res. Ctr. Internet & Tech. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (showing, for example, that while thirty-eight percent of adults were very confident or somewhat confident that their records held by credit card companies would remain private and secure, the corresponding figure dropped to eleven percent for social media sites).

[256]Speech of Commissioner Jourová, *supra* note 251.

[257]European Commission Press Release IP/18/4501, *The European Union and Japan Agreed to Create the World's Largest Area of Safe Data Flows* (July 17, 2018), http://europa.eu/rapid/press-release_IP-18-4501_en.htm.

throughout the United States.[258] As discussed in Part III.C., companies who meet the threshold requirements will need to provide certain protections to California consumers. This statute goes beyond the typical U.S. list of bits of data and provides a broad clause that states, "[p]ersonal information' means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[259] Essentially, as

[258]*See* Derek Hawkins, *The Cybersecurity 202: Why California Could Be the Bellwether for the Privacy Movement*, WASH. POST (June 29, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/06/29/the-cybersecurity-202-why-california-could-be-the-bellwether-for-the-privacy-movement/5b34d50e1b326b3967989d01/?noredirect=on&utm_term=.a39d44a25f77 (citing Nuala O'Connor, president of the Center for Democracy and Technology, for this proposition with respect to tech legislation).

[259]The statute goes on to provide a very inclusive list of examples of items that will be covered:

> Personal information includes, but is not limited to, the following:
> (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
> (B) Any categories of personal information described in subdivision (e) of § 1798.80.
> (C) Characteristics of protected classifications under California or federal law.
> (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
> (E) Biometric information.
> (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
> (G) Geolocation data.
> (H) Audio, electronic, visual, thermal, olfactory, or similar information.
> (I) Professional or employment-related information.
> (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g, 34 C.F.R. Part 99).
> (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

CaCPA, *supra* note 99, at § 1798.140(o)(1)(A)–(K) (2018).

In addition as tech companies, for example, prefer to self-regulate, it is very possible that a self-imposed compliance program that goes above and beyond what the GDPR requires will stave off federal regulators. Among other novel protections, the law stipulates that consumers have the right to request the deletion of personal information, opt out of the sale of personal information, and access the personal information in a readily useable format that enables its transfer to third parties without hindrance.

in the European model, the focus is on the potential harm that the release of such information can do rather than its category. By adopting this higher level of protection, these companies will save significant compliance costs down the road. Rather than dealing with the patchwork of regulation found in U.S. federal and state statutes, these companies can take a progressive approach anticipating what may become a worldwide standard.

Conclusion

There are substantial differences between the concept of personal information in the United States and the concept of personal data in the European Union. Protected PII in the United States covers a smaller set of information than the concept of personal data in Europe, although there is no harmonization of U.S laws in this regard. In light of the United States' move away from data protection, it seems unlikely that harmonization with European law will be established via treaty or statute. Companies may instead choose to self-regulate and get ahead of potential changes in privacy and data protection law in the United States and abroad.

Due to the extraterritorial effect of the GDPR, and because mechanisms permitting the transfer of data from the European Union to the United States incorporate the EU definition of personal data (such as in the Privacy Shield), companies still need to decide how they will handle the flow of data from the European Union as well as provide the protections required by the GDPR with respect to the data they collect and process. Much is at stake with potential fines amounting to billions of dollars and the possibility that personal data processing could be subject to an injunction by EU DPAs due to noncompliance.

Nonetheless, U.S. companies have choices when it comes to the handling of data. They can adopt separate compliance measures for users of their website based on the user's location or adopt a single platform for compliance. While various compliance options are available to companies, one has a clear strategic advantage: the adoption of one comprehensive privacy standard worldwide for the collection and processing of personal data. Since European privacy law is so influential worldwide and California is a harbinger of future legislation, by acting today to protect personal data in a manner consistent with the GDPR and the CaCPA, companies may better prepare for the regulatory landscape of

tomorrow and create efficiencies within their organizations. Companies can and should be proactive, instead of reactive. Furthermore, by demonstrating an ethical attitude toward the protection of data, companies that adopt such a comprehensive forward-thinking regulatory program can garner trust and encourage sales securing a better market position. In this spirit, compliance with the GDPR may no longer be deemed problematical or a costly burden, but rather a strategic legal pathway to obtain a trust-based form of competitive advantage.

APPENDIX

Comparison of protected information in the United States and the European Union[260]

	US Federal Law							
Sector	*Financial*	*Financial*	*Health*	*Children*	*Telecom*	*Telecom*	*Education*	*Video Rental*
Law	GLBA	FCRA	HIPAA	COPPA	CCA	TCA	FERPA	VPPA
Statute	1999 (15 U.S.C. § 6801)	1970 (15 U.S.C. § 1681)	1996 (42 U.S.C. § 201)	1988 (15 U.S.C. § 6501)	1984 (47 U.S.C. § 551)	1996 (47 U.S.C. § 222)	1974 (20 U.S.C. § 1232(g))	1988 (18 U.S.C. § 2710)
Applies to	Financial institutions	Consumer reporting agencies	Health plans, health care clearing houses, and health care providers	Any person who operates a website on the Internet or an online service	Cable operators	Telecommunications carriers	Educational agencies and institutions	Video tape service providers

(Continues)

[260]Excludes statutes focused on government.

	US Federal Law							
Sector	*Financial*	*Financial*	*Health*	*Children*	*Telecom*	*Telecom*	*Education*	*Video Rental*
Information protected	(A) The term "nonpublic personal information" means personally identifiable financial information— (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution. (15 U.S. C. 6809(4)(A))	The term "consumer report" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title. (15 U.S.C. § 1681(a))	The term "health information" means any information, whether oral or recorded in any form or medium, that—(A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. (42 U.S.C. § 262 ((4))	(8) The term "personal information" means individually identifiable information about an individual collected online, including—(A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph. (15 U.S.C. § 6501(8))	The term "personally identifiable information" does not include any record of aggregate data which does not identify particular persons. (47 U. S.C. § 551(a)(2) (A))	The term "customer proprietary network information" means— "(A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information." (47 U.S.C. § 222(f)(1))	(E) The term "personal information" means individually identifiable information including—(i) a student or parent's first and last name; (ii) a home or other physical address (including street name and the name of the city or town); (iii) a telephone number; or (iv) a Social Security identification number. (20 U.S.C. § 1232h(c)(6)(E))	The term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider. (18 U.S.C. § 2710(a)(3))

(Continues)

	EU Law
Sector	This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. (Art. 2(1))
Law	GDPR[261]
Regulation	Regulation 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1
Applies to	1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. (Art. 3)
Information protected	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); 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; (Art. 4(1))

[261] Note that in the case of telecommunications operators (now referred to as "providers of electronic communications services") in the European Union the ePrivacy Directive would also apply regarding information privacy. See Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of Nov. 25, 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 337) 11. Furthermore, a proposal for a regulation to replace the ePrivacy Directive is in the legislative process in the European Union. *See generally* W. Gregory Voss, *First the GDPR, Now the Proposed ePrivacy Regulation*, J. INTERNET L., July 2017, at 3 (describing ePrivacy law as a special law, complementing the general EU data privacy law—now, the GDPR—and the European Commission's proposal for an ePrivacy Regulation, which is still going through the legislative process).