Richmond Journal of Law & Technology Volume XXV, Issue 1

GDPR: THE END OF GOOGLE AND FACEBOOK OR A NEW PARADIGM IN DATA PRIVACY?

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

Cite as: 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).

* Kimberly A. Houser, Assistant Professor of Legal Studies, Oklahoma State University

** W. Gregory Voss, Associate Professor of Business Law, Toulouse Business School

The authors would like to thank Anjanette Raymond, Kelley School of Business, Indiana University, for her helpful comments.

ABSTRACT

EU Data Protection Agencies have been vigorously enforcing violations of regional and national data protection law in recent years against U.S. tech companies, but few changes have been made to their business model of exchanging free services for personal data. With the Cambridge Analytica debacle revealing how insufficient American privacy law is, we now find ourselves questioning whether the General Data Protection Regulation (GDPR) is not the onerous 99 article regulation to be feared, but rather a creation years ahead of its time. This paper will explain how the differences in U.S. and EU privacy and data protection law and ideology have led to a wide divergence in enforcement actions and what U.S. companies will need to do in order legally process the data of their users in the EU. The failure of U.S. tech companies to fulfill the requirements of the GDPR, which has extraterritorial application and becomes applicable on May 25, 2018, could result in massive fines (up to $4 billion using the example of Google). The GDPR will mandate a completely new business model for these U.S. tech companies that have been operating for well over a decade with very loose restrictions under U.S. law. Will the GDPR be the end of Google and Facebook or will it be embraced as the gold standard of how companies ought to operate?

TABLE OF CONTENTS

I. INTRODUCTION

[1] Recently, the world watched in both shock and amusement as Mark Zuckerberg tried to explain the Facebook business model to hopelessly out-of-touch U.S. Senators. Simply stated, Facebook and Google provide a free service to users in exchange for the use of their data.[1] The information is collected, categorized and analyzed in order to provide extremely targeted advertisements, the bread and butter of giant tech companies' business model.[2] The advertisers then gain access to this data.[3] Neither Google nor Facebook charge users for access to their platforms,[4] but they do charge advertisers for the access to the user profiles created.[5] While your name is not provided to the advertisers, a unique identifier is provided.[6] Although it

[1] *See* Chris J. Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 628 (2014).

[2] *See id.* at 608–09.

[3] *See* Selina Wang, *Twitter Sold Data Access to Cambridge Analytica-Linked Researcher*, BLOOMBERG (Apr. 29, 2018, 2:26 PM), https://www.bloomberg.com/news/articles/2018-04-29/twitter-sold-cambridge-analytica-researcher-public-data-access (last visited Oct. 22, 2018) (explaining that Facebook applications gain access to the data which can be used to target individuals on other platforms, and that while this data itself is not sold, as it is on platforms like Twitter, access to the data is sold and can be mined by third parties).

[4] *Cf.* Scott Cleland, *Why Google's Not a "Platform"*, FORBES (Oct. 19, 2011, 11:39 AM), https://www.forbes.com/sites/scottcleland/2011/10/19/why-googles-not-a-platform/#554e45ef6bbe [https://perma.cc/G2PG-S7VH] (discussing how Google offers free services that other platforms charge for users to access).

[5] *See generally* G.S. Hans, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era*, 19 MICH. TELECOMM. & TECH. L. REV. 163, 164 (2012) (discussing how exploiting and selling user data can be a lucrative business).

[6] *See* Mitchell Reichgut, *Advertiser ID Tracking and What it Means for You*, FORBES (May 16, 2016, 11:32 AM), https://www.forbes.com/sites/onmarketing/2016/05/16/advertiser-id-tracking-and-what-it-means-for-you/#5500800e18bf [https://perma.cc/678R-4VY7] ("Each smartphone is uniquely differentiated from hundreds of millions of other smartphones by something

is in Facebook and Google's financial interest to keep the contents of your unique identifier proprietary, data mining of their sites does occur and your data and unique identifier (if not your name, address, and most recent purchase) are collected and shared.[7]

[2] While this business model is legal in the U.S.,[8] the way these tech companies operate has long been a point of contention for European regulators. The Federal Trade Commission (FTC) is the administrative agency charged with protecting consumers against deceptive and unfair trade practices.[9] The FTC has brought only a handful of actions against companies such as Facebook and Google, but it is limited in what it can do because of the lack of omnibus privacy and data security legislation.[10] Most

called an ID. Google's version is known as GAID (Google Advertiser Identification) and Apple's is called IDFA (Identifier for Advertisers).").

[7] *See generally id.* (demonstrating that data can be vulnerable to outside parties, like advertising agencies).

[8] *See* Bob Sullivan, *'La Difference' Is Stark in EU, U.S. Privacy Laws*, NBC NEWS (Oct. 19, 2006, 11:19 AM), http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.W66ZZmhKhPY [https://perma.cc/KQD4-EXM6].

[9] *See About the FTC*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc [https://perma.cc/HN7Z-2V53].

[10] *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Approves Final Settlement with Facebook (Aug. 10, 2012) [hereinafter FTC August 10, 2012 Press Release], https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook [https://perma.cc/AQG5-HBMX] (discussing FTC settlement terms with Facebook); Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges that It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep [https://perma.cc/4QXD-L7PU] (discussing Facebook's 2011 settlement agreement with the FTC). *See generally* Complaint, *In re* Facebook, Inc., (F.T.C., 2012) (No. C-4365) (containing the FTC's complaint against Facebook); Decision and Order, *In re* Google, Inc., (F.T.C., 2011) (No. C-4336) (agreement containing FTC consent order with Google); Complaint, *In re* Twitter, Inc., (F.T.C., 2011) (No. C-4316) (containing the FTC's complaint against Twitter).

of the FTC's actions center on how these companies engaged in deceptive and unfair practices by misrepresenting their use and sharing of users' data.[11]

[3] On the other side of the Atlantic, European Union (EU) Data Protection Authorities (DPAs) have been actively and consistently enforcing regional and national privacy laws against these same companies. Hundreds of cases have been brought against U.S. tech companies by local DPAs,[12] but while most of these actions have resulted in finding that the tech companies have violated privacy and data security law, the consequence has predominantly been small fines due to the limits in the local regulations adopted pursuant to the European Data Protection Directive 95/46/EC (95 Directive).[13] This may all change in light of the

[11] *See What We Do*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/what-we-do [https://perma.cc/9VM4-45YQ].

[12] *See, e.g.*, *Global Data Protection Enforcement Report*, BAKER & MCKENZIE, https://globaltmt.bakermckenzie.com/data-protection-enforcement (last visited Oct. 24, 2018) (providing selected cases divided by jurisdiction). *See generally* Mark Jamison, *Five Reasons Why Europe Fines Google and the US Tech Sector*, AEIDEAS (July 23, 2018, 6:00 AM), http://www.aei.org/publication/five-reasons-why-europe-fines-google-and-the-us-tech-sector/ (explaining why the EU has pursued cases against U.S. tech companies).

[13] *See* Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. (L 281) [hereinafter 95 Directive]. In 2016, Google was fined €100,000 by the French data protection agency—*Commission Nationale de l'Informatique et des Libertés* (CNIL)—for failing to apply Europe's "right to be forgotten" law stemming from a 2014 ruling by the European Court of Justice (ECJ) which gave citizens the right to have internet search engines remove inaccurate or insufficient information about them from search results. *See* Sam Schechner, *France Fines Google Over Right to be Forgotten*, WALL STREET J. (Mar. 24, 2016, 6:28 PM), https://www.wsj.com/articles/france-fines-google-over-right-to-be-forgotten-1458847256 [https://perma.cc/HJM4-R7C5]. In 2017, Facebook was fined €150,000 by the CNIL for violating the French Data Protection Act, by collecting users' "personal data"—the European term that is similar to (but more expansive than) the U.S. term "personally identifiable information" (PII)—and using a cookie to obtain behavioral information, without adequately informing users. *See FACEBOOK Sanctioned for Several Breaches of*

EU's General Data Protection Regulation (GDPR),[14] which became applicable on May 25, 2018.[15] The GDPR, which replaces the 95 Directive, will allow European data protection authorities (DPAs) to fine companies up to the higher of €20,000,000 or 4 percent of their global turnover for the most serious category of data protection violations,[16] potentially increasing maximum fines to over $1 billion for a company such as Facebook and over $3 billion for one such as Google.

[4] Although the stated reasons for the passage of the GDPR are to harmonize laws across member states and to give users more control over their data,[17] it seems likely that this regulation is also intended to hold all companies in the tech field to the same standards. Because of the lax privacy and data security laws in the U.S., tech companies like Google and Facebook have become behemoths worldwide: Facebook has 66.25% of the market share of social media platforms[18] and Google has 92.74% of the market share of search engines.[19] There is a perception that these American

the French Data Protection Act, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (May 16, 2017), https://www.cnil.fr/en/facebook-sanctioned-several-breaches-french-data-protection-act [https://perma.cc/7MQ4-S5BN] (reporting on a sanction against Facebook imposed by CNIL for violating security law).

[14] Commission Regulation 2016/679, 2016 O.J. (L119) [hereinafter GDPR].

[15] *See id.* at arts. 94, 99.

[16] *See id.* at art. 83(5)–(6).

[17] *See Questions and Answers—Data Protection Reform Package*, EUROPEAN COMMISSION (May 24, 2017), http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm [https://perma.cc/Q26N-WURL].

[18] *See Social Media Stats Worldwide: Sept 2017–Sept 2018*, STATCOUNTER GLOBALSTATS, http://gs.statcounter.com/social-media-stats [https://perma.cc/94HD-HZHT] (down from 88% one year ago most likely due in part to the exposure of the connection between Facebook and Cambridge Analytica). Note that the top 4 U.S. social media companies dominate 95.86% of the world's social media market. *Id.*

companies have an unfair advantage because of the lax privacy laws in the U.S. as compared to the EU.[20] Members of the European Commission have indicated that the extraterritoriality of the GDPR will eliminate the unfair advantage that these U.S. tech companies enjoyed and will, at least with respect to users in Europe, open the way for European tech companies to compete on a level playing field.[21]

[5] The reason for the differences in these laws[22] and enforcement actions stems from the vastly different ideologies behind American and European data protection laws, which need to be understood in order to fully interpret European privacy and data protection laws. Because the EU is

[19] *See Social Engine Market Share Worldwide: Sept 2017—Sept 2018*, STATCOUNTER GLOBALSTATS, http://gs.statcounter.com/search-engine-market-share [https://perma.cc/4DDW-6ZC2].

[20] *Cf.* Florian Schaub, *Fragmented U.S. Privacy Rules Leave Large Data Loopholes for Facebook and Others*, SCI. AM. (Apr. 10, 2018), https://www.scientificamerican.com/article/fragmented-u-s-privacy-rules-leave-large-data-loopholes-for-facebook-and-others/ [https://perma.cc/BQB4-JMBB] (discussing why there is little incentive for American companies to protect U.S. consumers' privacy).

[21] *See Questions and Answers—General Data Protection Regulation*, EUROPEAN COMMISSION (Jan. 24, 2018), https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjmiI_SveDdAhVktlkKHQC4AzcQFjAAegQIAxAC&url=http%3A%2F%2Feuropa.eu%2Frapid%2Fpress-release_MEMO-18-387_en.pdf&usg=AOvVaw23q76MopyB9PEw4FLfTgoz [https://perma.cc/38LJ-WQV2].

[22] For a discussion of this in the context of sensitive consumer data and cloud computing, *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 (2013). With respect to the definition of personal data (and personally-identifiable information), *see* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877 (2014). For a more general comparative view, *see* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004); Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013).

setting a much higher standard in privacy and data protection law,[23] it is essential that U.S. companies take action now to comply with these requirements or potentially lose the ability to operate in the EU based on their current business model.[24] It is also likely that the Snowden revelations concerning the U.S. government's massive surveillance program, which led to invalidation of the Safe Harbor Framework that companies had relied on in order to allow cross-border transfers of personal data from the EU to the U.S., contributed to the shoring up of EU privacy and data security law and its application to players outside of the EU.[25]

[6] Data privacy is an important global social and economic issue. According to a PwC survey, 92% of American companies considered compliance with the GDPR a top priority in 2017;[26] however, it will require a massive paradigm shift for American companies trading in data. This paper will help enable a greater understanding of the differences between American and European privacy standards and what the GDPR will mean for U.S. companies, using Google and Facebook cases as examples.

---

[23] *See* GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES (2014) (pointing out the "major influence" of European data privacy standards worldwide, including Asia, and the "increasingly isolated position" of the United States); DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 995 (3rd ed. 2009) ("Outside of Europe, other countries from around the world are moving toward adopting comprehensive privacy legislation on the European model"); Griffin Drake, *Navigating the Atlantic: Understanding EU Data Privacy Compliance Amidst a Sea of Uncertainty*, 91 S. CAL. L. REV. 163, 175–76 (2017) (noting the trend toward following EU-style legislation but highlighting the examples of the United States and China as bucking this trend); Schwartz, *supra* note 22, at 1966–67 (noting the considerable impact of European law and the "relative lack of American influence").

[24] *See* Schwartz, *supra* note 22, at 1980 (2013).

[25] *See* Drake, *supra* note 23, at 164–65.

[26] *See GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey*, PWC (Jan. 23, 2017) [hereinafter *GDPR Compliance Top Priority*], https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html [https://perma.cc/X2E6-MUEX].

[7] In Section II, this paper will discuss current privacy and data security law in the EU and U.S. Section III will discuss prototypical enforcement actions against Google and Facebook for violating privacy and data security laws demonstrating the different handling in both the EU and U.S. Section IV will provide a summary of the provisions of the GDPR. Finally, Section V will provide guidance for compliance with the GDPR and what it means for U.S. tech companies.

II. PRIOR EU AND CURRENT U.S. PRIVACY AND DATA SECURITY LAW

[8] The right to data protection is one of the fundamental rights in the EU, and such rights are considered inalienable.[27] In the EU, this concept "appears to be grounded in the concept of human dignity,"[28] which highlights one of the differences between U.S. and EU law.[29] Although some EU member states began enacting privacy laws beginning in the 1970s,[30] the first attempt to harmonize laws throughout the EU was the 95 Directive which was replaced with the GDPR earlier this year.[31] The U.S., on the other hand, does not have any overarching federal privacy statute and handles privacy and data security on a sectoral basis.[32]

---

[27] *See* ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 240–41 (2015).

[28] *Id.* at 242.

[29] *See generally* Whitman, *supra* note 22, at 3–7 (highlighting the different attitudes between the U.S. and EU approaches to privacy) .

[30] *See, e.g.*, Arnaud G. Vanbremeersch & Christophe Clarenc, *France*, PRIVACY, DATA PROTECTION & CYBERSECURITY L. REV. (2017), https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151281/france [https://perma.cc/DW3S-64RN] (discussing data privacy evolution in France).

[31] *See* EU GDPR.ORG, https://eugdpr.org/ [https://perma.cc/SF87-NNNU].

[32] *See* Margot E. Kaminski, *When the Default is No Penalty: Negotiating Privacy at the NTIA*, 93 DENVER U. L. REV. 925, 926 (2016); *see also* Paul M. Schwartz, *The Value of Privacy Federalism*, *in* SOCIAL DIMENSIONS OF PRIVACY 324, 324–27 (Beate Roessler & Dorota Mokrosinska eds., 2015).

A. EU Privacy and Data Security Law

1. 95 Directive

[9] The 95 Directive was adopted by the EU to protect the privacy of personal data collected for or about natural persons, especially as it related to processing, using, or exchanging such data.[33] It was based on recommendations proposed by the Organisation for Economic Co-operation and Development (OECD), and was designed to harmonize data protection laws and establish rules for the transfer of personal data to *third countries* outside of the Union.[34] It resulted in the creation of DPAs in each of the OECD member states and charged them with creating and enforcing regulations to meet the privacy and data security requirements of the 95 Directive.[35] "Overall, the directive closely matched the recommendations of the OECD and the core concepts of privacy as a fundamental human right."[36]

[10] The OECD recommendations are founded on seven principles, which are numbered starting with seven in the text:

> 7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
> 8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

[33] *See Protection of Personal Data*, Summaries of EU Legislation: EUR-LEX, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14012, [https://perma.cc/ZHS4-NYZW]; *see also* 95 Directive, *supra* note 13, at recital 2.

[34] *See How Did We Get Here? – EUGDPR*, EUGDPR.ORG, https://eugdpr.org/the-process/how-did-we-get-here/ [https://perma.cc/H4PD-CGV8].

[35] *See id.*

[36] *See id.*

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the previous principle] except:
    a. with the consent of the data subject; or
    b. by the authority of law.
11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
13. An individual should have the right:
    a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
    b. to have communicated to him, data relating to him within a reasonable time;
       at a charge, if any, that is not excessive;
       in a reasonable manner; and
       in a form that is readily intelligible to him;
    c. to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
    d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.[37]

[11] The enforcement actions discussed in this paper were all brought under regulations member states adopted to comply with the 95 Directive.[38] The 95 Directive limited the transfer of data outside of the EU to countries whose laws provided adequate levels of protection for data (similar to the extent it is protected in the EU). [39]

2. Safe Harbor

[12] The United States and the European Union are each other's largest trade and investment partners with the trade in goods and services amounting to over $1 trillion dollar per year.[40] The 95 Directive limited the transfer of personal data outside of the EU to countries with an adequate

[37] *See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORG. ECON. COOPERATION & DEV., http://www.oecd.org/sti/ieconomy/oexcdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/W4VG-74QM].

[38] See *infra* Section III(A).

[39] Because the U.S. laws were considered inadequate, a cross border transfer document had to be negotiated between the EU and the U.S. *See* Commission Decision No. 2000/520/EC (*Safe Harbor*), 2000 O.J. (L 215) ¶¶ [1]–[7] [hereinafter Safe Harbor]. It was known as the Safe Harbor and is discussed in the next section. *See id.* at [9].

[40] In 2016, the figure that resulted from adding exports and imports between the United States and the European Union in both merchandise and services was €1.05 trillion. *See* Directorate-General for Trade, *USA Trade Statistics Overview*, EUROPEAN COMMISSION, http://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_111704.pdf [https://perma.cc/X6HW-UZEY]. Converted into dollars at the Treasury reporting rate of exchange as of year-end 2016, the figure is roughly $1.096 trillion. *See* Bureau of the Fiscal Service Funds Management Division, *Treasury Reporting Rates of Exchange as of December 31, 2016*, DEP'T TREASURY, https://www.fiscal.treasury.gov/fsreports/rpt/treasRptRateExch/itin-12-2016.pdf [https://perma.cc/7M49-J4B6].

level of protection of personal data,[41] unless a derogation applied.[42] Since information regarding European citizens could be transferred to and stored in or processed in the United States, there was a concern that the lax privacy laws in the United States were insufficient to protect European citizens from harm.[43] Because the U.S. did not meet the EU's required standard of protection, the Safe Harbor agreement was negotiated between the two blocks to allow for U.S. companies to transfer personal data to the U.S.[44] The Safe Harbor agreement provided that if U.S. companies receiving data transfers agreed to comply with the standards contained therein, and self-certified as compliant, they were safe from data protection law enforcement action by European DPAs, because enforcement actions would be taken by the FTC for noncompliance with the agreement.[45]

[13] In recent years, cross-border data flow has expanded exponentially due to the widespread use of the Internet. The 95 Directive was intended to address concerns with the flow of information to companies outside of the European Union.[46] It defined the "data controller" as an entity that determines the purposes and means of the collection and processing of the

[41] *See* 95 Directive, *supra* note 13, at art. 25(1).

[42] *See id.* at art. 26(1).

[43] *See* Klint Finley, *Thank (or Blame) Snowden for Europe's Big Privacy Ruling*, WIRED (Oct. 6, 2015 9:06 PM), https://www.wired.com/2015/10/tech-companies-can-blame-snowden-data-privacy-decision/ [https://perma.cc/JU4F-W3TJ].

[44] *See id.*

[45] *See* Safe Harbor, *supra* note 39, at ¶¶ [1]–[7]. Nonetheless, the EU data controller was still subject to the provisions of the 95 Directive and as such subject to the jurisdiction of one or more DPAs in the European Union (which could include the EU subsidiary of a U.S. firm, or could even extend to a U.S. firm found to have an establishment in the European Union, in certain circumstances). *See id.* at Annex II, FAQ 10. *See generally* 95 Directive, *supra* note 13 (outlining duties of data controllers).

[46] Indeed, within the EU, the 95 Directive and the GDPR are meant to ensure the free-flow of data given the harmonized level of protection throughout the EU. *See* GDPR, *supra* note 14 at art. 1(3).

information[47] and the "processor" as the party that processes the information on behalf of the controller[48] As a practical matter, when speaking of cross-border transfers under the 95 Directive, the controller is usually located within the European Union, and is transferring personal information outside of the European Union for processing.[49] The controller is clearly bound to respect the laws of the European Union, but the receiving American companies have argued that the laws do not apply to the processor located in the United States.[50] The Safe Harbor agreement remained in place until the European Court of Justice invalidated the agreement, in large part due to the Snowden revelations regarding the U.S. government's monitoring and secret collection of information.[51] Its replacement, the Privacy Shield, is discussed in Section IV(C)(1) below.

B. U.S. Privacy and Data Security Law

1. Federal Privacy Law

[14] Unlike EU data protection law, U.S. privacy law is handled on a sectorial basis.[52] The handling and processing of personal data is regulated

[47] The 95 Directive defines "controller" as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." 95 Directive, *supra* note 13, at art. 2(d). The corresponding definition in the GDPR remains largely the same. *See* GDPR, *supra* note 14, at art. 4(7).

[48] *See* 95 Directive, *supra* note 13, at art. 2(e); *see also* GDPR, *supra* note 14, at art. 4(8) (defining "processor" as a "natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controllers").

[49] *See* 95 Directive, *supra* note 13, at recitals 56–57.

[50] *See* Schwartz, *supra* note 22, at 1995, 2003.

[51] *See* MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RESEARCH SERV., R44257, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 1 (2016).

[52] *See* Lisa J. Sotto & Aaron P. Simpson, *United States*, *in* DATA PROTECTION & PRIVACY 191 (Rosemary P. Jay ed. 2014),

by both states and the federal government, but for the most part, relates to the specific category of information at issue.[53] The categories covered under federal law are healthcare data (under the Health Information and Portability Accountability Act, HIPAA),[54] financial data (under the Gramm Leach Bliley Act, GLB)[55] children's information (under the Children's Online Privacy Protection Act, COPPA),[56] students' personal information (under Family Educational Rights and Privacy Act, FERPA),[57] and consumer information (under the Fair Credit Reporting Act, FCRA);[58] but, significantly, these statutes were enacted prior to significant personal use of the Internet.[59] The main regulatory body addressing privacy breaches is the

https://www.huntonak.com/images/content/3/3/v3/3351/United-States-GTDT-Data-Protection-and-Privacy-2014.pdf [https://perma.cc/X2W9-YS23].

[53] *See id*.

[54] *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 115-244, 110 Stat. 1936.

[55] *See* 15 U.S.C. § 6801 (2018).

[56] *See* 15 U.S.C. § 6502 (2018).

[57] *See* 20 U.S.C. § 1232(g) (2018).

[58] *See* 15 U.S.C. § 1681 (2018).

[59] HIPAA was enacted in 1996, GLB in 1999, COPPA in 1998, FERPA in 1974, and FCRA in 1970. *See When was HIPAA Enacted?*, HIPAA J. (Mar. 9, 2018), https://www.hipaajournal.com/when-was-hipaa-enacted/ [https://perma.cc/BTF6-CEZ4]; Margaret Rouse, *Definition: Gramm-Leach-Bliley Act (GLBA)*, TECHTARGET, https://searchcio.techtarget.com/definition/Gramm-Leach-Bliley-Act [https://perma.cc/R664-SWZR]; Jeff Knutson, *What is COPPA?*, THE J. (Mar. 5, 2018), https://thejournal.com/articles/2018/03/05/what-is-coppa.aspx [https://perma.cc/DB89-C75Q]; Pam Dixon, Student *Privacy 101: What is FERPA and Why Does It Matter?*, WORLD PRIVACY FORUM (Jan. 20, 2015), https://www.worldprivacyforum.org/2015/01/a-brief-history-of-ferpa-reform-and-why-it-matters/ [https://perma.cc/V9RB-RQZN]; Jake Stroup, *The Fair Credit Reporting Act of 1970*, THE BALANCE, https://www.thebalance.com/fair-credit-reporting-act-of-1970-1947567 [https://perma.cc/TA59-U5X9]. In comparison, Facebook was not launched until 2004. *See* Sarah Phillips, *A Brief History of Facebook*, THE GUARDIAN (July 25,

FTC.[60] The FTC was not specifically charged to enforce privacy policies, but it is responsible for taking action against companies engaged in unfair and deceptive trade practices.[61] Although there is no federal legal requirement in the U.S. for Internet service providers to maintain privacy policies informing users how their information will be used, nor are companies required to obtain permission to use the data, companies that do supply privacy policies can be subjected to action for failing to comply with them or otherwise misleading the public.[62]

[15] One of the reasons why the FTC got involved in regulating privacy issues at the time it did was that the 95 Directive was going into effect and it would require the U.S. to have "adequate" privacy protections before personal data could be transferred from the European Union to America.[63] At the time no enforcement body existed in the U.S. to ensure compliance with the Safe Harbor agreement, so Congress convinced the FTC to take on this role.[64] However, it was not until March 2012, that the FTC came out with its Recommendations for Businesses and Policymakers to address the

2007, 5:29 EDT), https://www.theguardian.com/technology/2007/jul/25/media.newmedia [https://perma.cc/CMQ4-ZTK5].

[60] *See Division of Privacy and Identity Protection*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity [https://perma.cc/3ZE8-F93D] (explaining the responsibilities of Federal Trade Commission as they relate to privacy breaches).

[61] *See Privacy and Security Enforcement*, FED. TRADE COMMISSION., https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises [https://perma.cc/F93N-E8YS].

[62] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and The New Common Law of Privacy*, 114 COLUM. L. REV. 583, 588 (2014).

[63] *See* David L. Baumer et al., *Internet Privacy Law: A Comparison Between the United States and the European Union*, 23 COMPUTERS & SECURITY 400, 408 (2004).

[64] *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 145–46, 159 (2016).

issue of consumer privacy.[65] While this report provided guidance for businesses, it did not mandate any particular action.[66] As privacy scholars Solove and Hartzog point out, there is virtually no case law on FTC privacy enforcement actions because nearly all of them have resulted in settlements between the FTC and the companies investigated.[67] This also means that the companies seldom had to admit to any wrongdoing.[68] These privacy enforcement actions are discussed more fully in Section III(B) below.

2. State Data Protection Law

[16] Although the FTC has brought a number of actions involving data breaches by companies, most of these fall under one of the above-mentioned sector-specific statutes, or under section 5 of the FTC Act regarding unfair and deceptive trade practices.[69] Additionally, very few class-action cases have made it to court due to the lack of harm being shown with a data breach.[70] The FTC Act does not permit private causes of action.[71] One statute that has been used successfully to certify a class action, has been the

[65] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICY MAKERS (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/FCD2-P8EY].

[66] *See id.* (the report does, however, acknowledge the need for Congress to set baseline privacy protection laws).

[67] *See* Solove & Hartzog, *supra* note 62, at 585.

[68] *See id.* at 610.

[69] *See id.* at 585–87.

[70] *See* Timothy H. Madden, *Data Breach Class Action Litigation—A Tough Road for Plaintiffs*, 55 BOSTON BAR J. 27, 27–28 (2011).

[71] *See, e.g.*, Days Inn of Am. Franchising, Inc. v. Windham, 699 F. Supp. 1581, 1582 (N.D. Ga. 1988).

Stored Communications Act.[72] Facebook settled a class action suit for $9.5 million in *Lane v. Facebook, Inc.*, with respect to its ill-fated Beacon program which automatically posted user's offsite platform activities to their Facebook newsfeed (such as the purchase of theater tickets).[73] In *Lane*, the plaintiffs alleged that Facebook had violated both California and federal law, including the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, the Video Privacy Protection Act, California's Computer Crime Law, and the California Consumer Legal Remedies Act.[74] However, it should be noted that most cases for data breaches and tort actions have not been as successful because many courts require a showing of harm.[75] In *Spokeo, Inc. v. Robins,* the Supreme Court indicated that the plaintiff lacked standing because of the absence of actual injury due to the data breach.[76] The majority of cases regarding data breaches are pursued under state law.[77]

[17] All 50 states have enacted data breach notification statutes, following the lead of California's 2003 statute.[78] California's statute

[72] *See, e.g.*, Gaos v. Holyoak., 869 F.3d 737, 739–40, 747 (N.D. Cal. 2017) (affirming the *cy pres* settlement of a class action brought under the Stored Communications Act).

[73] *See* Lane v. Facebook, Inc., 696 F.3d 811, 816–17 (9th Cir. 2012) (stating that Beacon was shut down after two years in 2009).

[74] *See id*. at 816 n.1.

[75] *See* Madden, *supra* note 70 at 27–30.

[76] *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1544, 1550 (2016) (stating that Robins, the plaintiff, alleged that Spokeo, a "people search engine," disclosed incorrect information about Robins in violation of the Fair Credit Reporting Act).

[77] *See generally* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 206–208 (2017) (providing a detailed list of state data breach notification laws).

[78] *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/ [https://perma.cc/ZQG9-VUYZ].

requires notification to individuals if their personal information has been released.[79] The California statute defines "personal information" as a person's first name or initial and last name combined with any one or more of the following: "social security number; driver's license number or [state] identification card number; account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;" as well as medical information and health insurance information.[80] The state statutes vary widely on what constitutes a data breach, and when and if users need to be notified.[81]

C. Differences Between EU and U.S. Laws

[18] Data privacy is a global issue because companies operate across borders.[82] It is vital that they understand the privacy and data protection laws in the countries with which they do business.[83] The United States and

[79] *See Data Security Breach Reporting*, ST. CAL. DEP'T JUST. OFF. ATT'Y GEN., https://oag.ca.gov/privacy/databreach/reporting [https://perma.cc/ZN9J-QAFA].

[80] *See* CAL. CIV. CODE § 1798.29(g) (West 2010).

[81] *See* Dana Lesemann, *Once More Unto the Breach: An Analysis of Legal, Technological and Policy Issues Involving Data Breach Notification Statutes*, 4 AKRON INTELL. PROP. J. 203, 213 (2010).

[82] The United States and the European Union remain each other's largest trade and investment partners with the trade in goods and services amounting to over $1 trillion dollar per year. *See* WEISS & ARCHICK, *supra* note 51, at 4. In addition, cross-border data flows between the United States and Europe are the highest in the world—almost double the data flows between the United States and Latin America and 50% higher than data flows between the United States and Asia. *See* Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment*, GLOBAL ECON. & DEV. BROOKINGS (Oct. 2014), https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf [https://perma.cc/DYZ3-HZKZ].

[83] *See* Andre R. Jaglom, *Liability On-Line: Choice of Law and Jurisdiction on the Internet, or Who's In Charge Here?*, 16 INT'L L. & PRAC. SEC. NYSBA 12 (2002), http://www.thsh.com/documents/liabilityon-line.pdf [https://perma.cc/4GKM-BF6N].

the European Union are each other's largest trade and investment partners.[84] However, there are striking differences between European and American privacy laws.[85] While the European Union focuses on protecting human rights and social issues, the U.S. seems to be concerned with providing a way for companies collecting information[86] to use that information while balancing the privacy rights that consumers expect.[87] Although data protection and privacy are important issues for consumers, as the Cambridge Analytica hearings demonstrated, the U.S. does not provide adequate privacy and data security protection.[88] While Facebook founder Mark Zuckerberg was brought to task for *allowing* Cambridge Analytica to happen, the Senate demonstrated its complete lack of understanding of modern technology and it is woefully ill-equipped to create adequate privacy and data security laws.[89] It seems that Congress is relying on the

[84] *See* Gilberto Gambini et al., *Archive: USA-EU-International Trade and Investment Statistics: EU & US Form the Largest Trade and Investment Relationship in the World*, EUROSTAT STAT. EXPLAINED (last updated Jan. 5, 2018, 15:27), https://ec.europa.eu/eurostat/statistics-explained/index.php?title=USA-EU_-_international_trade_and_investment_statistics&oldid=368909 (last visited Oct. 26, 2018).

[85] *See* Edward R. Alo, *EU Privacy Protection: A Step Towards Global Privacy*, 22 MICH. ST. INT'L L. REV. 1095, 1101, 1104, (2013).

[86] According to a Congressional Research Service Report, "The U.S. Department of Commerce recently reiterated that the large-scale collection, analysis, and storage of personal information is central to the Internet economy; and that regulation of online personal information must not impede commerce." GINA STEVENS, CONG. RESEARCH SERV., R41756, PRIVACY PROTECTIONS FOR PERSONAL INFORMATION ONLINE 2 (2011).

[87] *See* Gry Hasselbalch & Pernille Tranberg, *Data Monopolies and Value Clashes*, DATA ETHICS (May 19, 2017), https://dataethics.eu/en/data-monopolies-value-clashes/ [https://perma.cc/KL8P-6UYK].

[88] *See* S. COMM. ON THE JUDICIARY & S. COMM. ON COM., SCI., AND TRANSP., 115th CONG., *Facebook, Social Media Privacy, and the Use and Abuse of Data* (April 10, 2018, 2:15 PM).

[89] *See id.*

FTC to use Article 5 (regarding deceptive and unfair trade practices) to monitor and enforce privacy and data security in the U.S.

[19] The vast differences between U.S. and EU privacy law directly relates to the differences in the respective ideologies behind these laws. [90] While the U.S. Constitution does not mention a right to privacy,[91] it is expressly included in the Charter of Fundamental Rights of the European Union.[92] The Charter of Fundamental Rights, whose rights, freedoms, and principles were recognized as having the same value as the European Union

[90] *See* Alo, *supra* note 85, at 1101, 1104.

[91] As pointed out by one scholar, "The word "privacy" does not appear in the United States Constitution. Yet concepts of private information and decisionmaking are woven through the entire document, and courts have developed a substantial jurisprudence of constitutional privacy." WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 3 (2016); s*ee also*, ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY xiii (1995) (discussing The Bill of Rights and a shrinking right to privacy). This having been said, one 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: THE DESTRUCTION OF PRIVACY IN AMERICA 5 (2011). 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 23, at 2. In 1890, Warren and Brandeis made the argument in the Harvard Law Review that the right of privacy is implied by the constitution and derived from both common law and the concepts of "the right to be left alone" and the right to keep personal information out of the public domain. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV.L. REV. 193, 193 (1890),. This right to privacy has been adopted by the Supreme Court and throughout the states. *See* William M. Beaney, *The Constitutional Right to Privacy in the Supreme Court*, 1962 SUP. CT. REV. 212, 212–13.

[92] Article 8(1) of the Charter of Fundamental Rights of the European Union, provides that: "Everyone has the right to the protection of personal data concerning him or her." Charter of Fundamental Rights of the European Union art. 8(1), 2000 O.J. (C 364) 1, 10. In addition to protecting the personal information of those in the European Union, it also protects their right to private or family life. *Id*. art. 7, at 10.

treaties[93] (Treaty on European Union[94] and Treaty on the Functioning of the European Union[95]), and its treatment of personal data protection as a fundamental right, represent the vast difference between how the United States and the European Union view personal information and, as a result, the policy behind their respective privacy laws. For example, in the European Union, unless some other legal basis for processing personal data applies (e.g., processing is necessary for performance of a contract to which the data subject is a party),[96] companies that provide online services to residents of the European Union can be required to obtain documented *hard consent* from customers before processing and storing their data.[97] This is the exact opposite of what U.S. companies do.[98] Rather than requiring users to opt in to the sharing of their personal information, people using U.S. tech companies' services must actively opt out, or in the alternative stop using the service.[99] In addition, U.S. law does not prevent companies from sharing the information they collect with third parties, provided such activities are

[93] *See* Consolidated Version of the Treaty on European Union, art. 6(1) 2012 O.J. C 326 13, 19.

[94] *Id.*

[95] *See* Consolidated Version of the Treaty on the Functioning of the European Union, Oct. 26, 2012, 2012 O.J. C 326 47

[96] *See* GDPR, *supra* note 14, at art. 6(1)(b).

[97] *See* Allison Grande, *Cybersecurity Policy to Watch for the Rest of 2017*, LAW360 (July 12, 2017, 7:47 PM), https://www.law360.com/articles/937323/cybersecurity-policy-to-watch-for-the-rest-of-2017 [https://perma.cc/PNF9-3DM3].

[98] *See generally* FED. COMM. COMMISSION, FCC 16-148, PROTECTING THE PRIVACY OF CUSTOMERS OF BROADBAND AND OTHER TELECOMMUNICATIONS SERVICES, 13963 (Oct. 27, 2016) (stating that, for example, the GLBA only requires financial institutions provide customers an opportunity to opt out from the sharing of their nonpublic personally identifiable customer information with non-affiliated third parties). *See also* Anne T. McKenna, *Pass Parallel Privacy Standards or Privacy Perishes*, 65 RUTGERS L. REV. 1041, 1077–78 (2013) (noting that U.S. companies' privacy policies do not allow any amount of choice).

[99] *See* McKenna, *supra* note 98, at 1077.

disclosed.[100] This means consent is not required under U.S. law for secondary uses of data.[101] As the next section will demonstrate, U.S. companies have been running afoul of European privacy law for over a decade.

III. ENFORCEMENT ACTIONS AGAINST U.S. TECH COMPANIES

A. EU Enforcement Actions

[20] Over the past decade, EU member state DPAs have brought enforcement actions against major U.S. technology companies for privacy law violations.[102] In this section we consider several of these cases, focusing on those involving Google and Facebook as being representative of the types of actions brought concerning privacy law.

1. Google

a. Google Street View Privacy Case

[21] In 2007, Google launched its Street View program in the U.S. whereby vehicles were fitted with cameras and other equipment to take panoramic photographs along roadways to complement its Google maps app.[103] In addition to photographing images of houses and businesses along

[100] *See* Clark D. Asay, *Consumer Information Privacy and Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 324, 326, 330, 338 (2013).

[101] *See id.* at 337, 343.

[102] *See* Richard K. Clark, *What Will U.S. Companies Have to Do to Comply with the EU Privacy Shield Agreement?*, LEWIS ROCA ROTHGERBER CHRISTIE, LLP (Apr. 7, 2016), https://www.lrrc.com/client-alert-what-will-us-companies-have-to-do-to-comply-with-the-eu-privacy-shield-agreement [https://perma.cc/9AAE-QLXN].

[103] *See* Tom Simonite, *Google's New Street View Cameras Will Help Algorithms Index the Real World*, WIRED (Sept. 5, 2017, 7:00 AM) https://www.wired.com/story/googles-new-street-view-cameras-will-help-algorithms-index-the-real-world/ [https://perma.cc/LL2T-9MZ5].

these roadways, the vehicles picked up GPS data, wi-fi network names, and possibly content from open wireless networks.[104] Google eventually admitted to having "been mistakenly collecting samples of payload data from open networks," which may have included e-mail, text, photographs, or even websites that people were viewing, while its Street View cars were traveling around taking photographs.[105] This collection of data was discovered after German authorities asked to audit the cars because homeowners feared that images of their domiciles could lead to burglary.[106] As a result, Google agreed to allow houses to be blurred out of images on request (by opting out).[107] At the time, all 27 European member states had created data protection laws derived from the 95 Directive.[108] Although the laws varied from jurisdiction to jurisdiction, they all prohibited the interception of personal data, and in some member states, made it a criminal offense.[109] Germany issued a fine against Google for $189,000 as a result of their data privacy violation.[110] The capturing of data by Google Street View resulted in similar EU member state DPA enforcement actions in

[104] *See* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA 108 (2014).

[105] *See* Maggie Shiels, *Google Admits Wi-Fi Data Collections Blunder,* BBC NEWS (May 15, 2010, 12:29 AM), http://news.bbc.co.uk/2/hi/technology/8684110.stm [https://perma.cc/7KZA-XVGH].

[106] *See id*.

[107] *See* MAYER-SCHÖNBERGER & CUKIER, *supra* note 104, at 153.

[108] *See* Andrea Ward & Paul Van den Bulck, *Differing Approaches to Data Protection/Privacy Enforcement and Fines, Through the Lens of Google Street View*, IAPP: THE PRIVACY ADVISOR (June 1, 2013), https://iapp.org/news/a/2013-06-01-differing-approaches-to-data-protection-privacy-enforcement-and/ [https://perma.cc/YJ7U-QXHT].

[109] *See id.*

[110] *See* Aaron Souppouris, *Google Fined Just $189,000 for 'One of the Biggest' Data Protection Violations in German History,* THE VERGE (Apr. 22, 2013, 7:49 PM) https://www.theverge.com/2013/4/22/4251768/google-germany-street-view-data-protection-wi-fi-fine [https://perma.cc/J2RZ-6H8U].

Europe[111] and various other nations worldwide.[112] Belgium settled with Google for €150,000 in April 2011, to close charges on the company's unauthorized collection of private data from unencrypted wi-fi networks.[113] The French *Commission Nationale de l'Informatique et des Libertés* (CNIL), the DPA in France, sanctioned Google Street View's collection of personal data on March 17, 2011, in what then was a record fine of €100,000.[114]

[22] The failure by Google to provide adequate information to the data subjects about the processing of their data also violated French law.[115] A report regarding the CNIL press release on the case indicated "that inspections carried out by the CNIL in late 2009 and early 2010 demonstrated that vehicles (Google Street View cars used for Google Maps services) deployed on the French territory collected and recorded not only

[111] *See* Press Release, Fed. Data Prot. and Info. Comm'r (FDPIC), Judgment in Google Street View Case: Court Finds in Favour of the FDPIC (Apr. 4, 2011), https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2011/04/medienmitteilungzumurteildesbundesverwaltungsgerichtsinsachengoo.pdf.download.pdf/press_release_verdictofthetribunaladministrativfederalingooglest.pdf [https://perma.cc/Z6PY-Y3P3].

[112] *See Investigations of Google Street View*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/streetview/ [https://perma.cc/CQL6-GN3P].

[113] *See* Ward & Van den Bulck, *supra* note 108.

[114] The CNIL found that SSID information and MAC addresses collected by Google allowed identification of data subjects if combined with other location data collected, and that the same was true of "payload data" that Google had inadvertently collected as well. The significance of such data allowing identification is that it would then be considered "personal data" meaning that EU data protection law obligations, as implemented in member state law, would apply to its processing. *See* Myria Saarinen, *France's CNIL Announces a Record Fine of €100,000*, LEXOLOGY (Mar. 28, 2011), https://www.lexology.com/library/detail.aspx?g=967da607-a9a1-41f9-a082-5fb0dbbed204 [https://perma.cc/BPG8-EEFQ].

[115] *See id.*

photographs but also data transmitted by individuals' wireless Wi-Fi networks without their knowledge."[116]

[23] The Netherlands DPA—*College Bescherming Persoonsgegevens*—issued an order against Google on March 23, 2011 in connection with violations related to Google Street View, as a result of

> an investigation [that] indicated that the company had used its Street View vehicles to collect data on more than 3.6 million Wi-Fi routers in the Netherlands, both secured and unsecured, during the period March 4, 2008, to May 6, 2010, and had also calculated a geolocation for each router. Such acts constituted a violation of the PDPA [the Dutch Personal Data Protection Act]. According to a DPA press release, "MAC [media access control] addresses combined with a calculated geolocation constitute personal data in this context, because the data can provide information about the owner of the WiFi router in question."[117]

The order could have resulted in a fine up to €1 million against Google,[118] but Google was able to avoid it by complying.[119] Google was also more

[116] Nicole Atwill, *France*, *in* ONLINE PRIVACY LAW: AUSTRALIA, CANADA, FRANCE, GERMANY, ISRAEL, ITALY, JAPAN, NETHERLANDS, PORTUGAL, SPAIN, SWEDEN, & THE UNITED KINGDOM, 40, 53 (L. Libr. Congress ed. 2012), https://www.loc.gov/law/help/online-privacy-law/online-privacy-law.pdf [https://perma.cc/X96F-L6DT].

[117] Wendy Zeldin, *Netherlands*, *in* ONLINE PRIVACY LAW, *supra* note 116, at 129, 146.

[118] *See* Press Release, Autoriteit Persoonsgegevens, Dutch DPA Issues Several Administrative Orders Against Google (Apr. 19, 2011), https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-issues-several-administrative-orders-against-google [https://perma.cc/5G4Z-TWJY].

[119] *See* Stephen Gardner, *Dutch DPA Concludes That Google Is in Breach of Data Protection Act*, BLOOMBERG LAW (Dec. 2, 2013), https://www.bna.com/dutch-dpa-concludes-n17179880411/# [https://perma.cc/66Q3-44ZA].

recently fined $1.4 million by Italy for its Google Street View's privacy violations.[120]

b. Google Privacy Policy Case

[24] The first set of EU DPA Google privacy policy enforcement actions against Google came as a result of revisions made to the latter's privacy policy in March 2012.[121] Google indicated that it was going to consolidate all of its some 70 products' privacy policies into one.[122] However, this new policy would allow it to share data between companies and products.[123] In response to this change, the Article 29 Data Protection Working Party (WP 29), which was an influential advisory group that included representatives of EU member state DPAs,[124] made recommendations to Google for

[120] *See Google Pays 1-Million-Euro Fine Imposed by the Italian DPA Because of Google's Street View Service*, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (April 3, 2014), http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3041085 [https://perma.cc/MF6Z-3RAH].

[121] Letter from Article 29 Data Protection Working Party to Larry Paige, Chief Executive Officer, Google Inc. (Oct. 16, 2012), https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20121016_letter_to_google_en.pdf [https://perma.cc/5UCN-HZ32].

[122] *See Google to Change Privacy Policy After ICO Investigation*, INFO. COMMISSIONER'S OFF. (Jan. 30, 2015), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/01/google-to-change-privacy-policy-after-ico-investigation/ [https://perma.cc/LD3W-2V39].

[123] *See* Mark Hachman, *Google Overhauls, Consolidates Privacy Policies*, PC MAG (Jan. 24, 2012, 8:59 PM), https://www.pcmag.com/article2/0,2817,2399308,00.asp [https://perma.cc/G6ND-25C9?type=image].

[124] WP 29 was created under the 95 Directive. *See* 95 Directive, *supra* note 13, at art. 29. On May 25, 2018 it was replaced by the European Data Protection Board, established pursuant to the GDPR. *See* GDPR, *supra* note 14, at art. 68(1). *See also The Article 29 Working Party Ceased to Exist as of 25 May 2018*, EUR. COMM'N JUSTICE AND CONSUMERS (June 11, 2018), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492 [https://perma.cc/Y8MM-XA97].

modifications to its practices and its privacy policy to bring them into compliance.[125] When Google failed to make the recommended changes to its practices and policy,[126] a number of DPAs brought enforcement actions against Google for violating member state law which required data controllers to obtain user consent to the sharing of their information across companies and products, among other violations.[127] France ordered Google to (1) define the specific purposes of processing users' personal data, (2) define retention periods for personal data not to exceed the period necessary for the purposes collected, and (3) inform users and obtain consent prior to storing cookies on their devices.[128] Similarly, five other DPAs have cited Google for failing to comply with similar provisions of their data protection legislation.[129] Google's failure to comply resulted in a €150,000 fine by the

[125] *See* Letter from Article 29 Data Protection Working Party to Larry Paige, Chief Executive Officer, Google Inc. (Sept. 23, 2014) [hereinafter Article 29 Letter Sept. 23, 2014] https://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy.pdf [https://www.perma.cc/843K-XSWY].

[126] *See The Google Privacy Investigation in Europe: Two Years On*, INITIATIVE FOR A COMPETITIVE ONLINE MARKETPLACE, http://i-comp.org/wp-content/uploads/2014/10/The-Google-Privacy-Investigation-in-Europe-Two-Years-On4.pdf [https://perma.cc/RGB4-84RW]

[127] The enforcement action was taken by the DPAs of France, Germany, Italy, the Netherlands, Spain, and the United Kingdom. *See* W. Gregory Voss, *European Union Data Privacy Law Developments*, 70 BUS. LAW. 253, 254 (2014) [hereinafter Voss, *Data Privacy Law*]. In addition, the UK's DPA ordered Google to sign a consent decree improving the way it collected personal information in the UK. *See* Brian Davidson, *UK—Google To Change Privacy Policy After ICO Investigation*, IAPP (Feb. 24, 2015), https://iapp.org/news/a/ukgoogle-to-change-privacy-policy-after-ico-investigation/ [https://perma.cc/SX9N-ZV8F].

[128] *See* Lance Whitney, *France Orders Google to Change its Privacy Policies*, CNET (June 20, 2013, 6:33 AM), https://www.cnet.com/news/france-orders-google-to-change-its-privacy-policies/ [https://perma.cc/7ZYU-KUHW?type=image].

[129] *See* Voss, *Data Privacy Law*, *supra* note 127, at 255.

CNIL.[130] In addition, Google was ordered to cease its personal data processing and to publish the order and fine on its French home page for 48 hours.[131]

[25] The second set of enforcement actions as a result of the 2012 privacy policy changes were instituted by the Italian DPA in 2014 for violation of Italian law, and ordered Google to provide more "effective information notices" to it users[132] and to obtain prior consent from its users for the processing of their personal information. [133] This included both users of Gmail and Google Search.[134] It was discovered that Google was processing information in users' Gmail accounts for the purposes of behavioral advertising [135] by using cookies and engaging in other profiling activities in order to create targeted ads.[136] The order also set forth time frames for which

[130] *See id.* at 254-55.

[131] *See* Commission Nationale de l'Informatique et des Libertés, *Délibération n°2013-420 de la Formation Restreinte Prononçant une Sanction Pécuniaire à l'Encontre de la Société X* (Deliberation No. 2013-420 of the Sanctions Committee of CNIL Imposing a Financial Penalty Against Company X), LEGIFRANCE (Jan. 3, 2014), http://goo.gl/exjL12 [https://perma.cc/QT85-ZVXK]. The decision has now been rendered anonymous and Google Inc. is referred to as "Société X" (Company X). *See generally* Voss, *Data Privacy Law*, *supra* note 127, at 255–257 (discussing similar fines imposed by Spanish, Italian, and Dutch DPAs).

[132] *See Decision Setting Forth Measures Google Inc. Is Required to Take to Bring the Processing of Personal Data Under Google's New Privacy Policy into Line with the Italian Data Protection Code*, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (July 10, 2014) [hereinafter *Measures Google Inc. Is Required to Take*], http://goo.gl/EgAT1x [https://perma.cc/6B9B-T8JD].

[133] *See id.*

[134] *See id.*

[135] *See id.*

[136] *See id.* It should also be noted that the definition of "processing" (or "processing of personal data") is very broad in the 1995 Directive: "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as

Google was to respond to data deletion requests by authenticated users holding Google accounts, where the user requested deletion of his or her data in accordance with data protection law.[137]

[26] In 2014, the Hamburg DPA, acting for Germany, also issued an order noting Google's violations of German data protection law with respect to its data processing activities and user profiling, such as the use of the substantial information Google collects about users' habits combined with other information Google obtains, such as location data.[138] Then on September 23, 2014, the WP 29 confirmed the findings of a meeting between the WP 29, Google, and the above-mentioned DPAs summarizing

collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." 95 Directive, *supra* note 13, at art. 2(3).

[137] *See Measures Google Inc. Is Required to Take*, *supra* note 132. The decision specifically carves out "right to be forgotten" deletion requests, and in the grounds for the decision, the Italian DPA refers to the *Google Spain* case, as well as guidelines then to come from the Article 29 Data Protection Working Party for treatment of "right to be forgotten" deletion requests, stating that "the Garante will limit itself, at this stage, to issuing specific instructions with regard to data deletion requests lodged by . . . users holding Google accounts . . . [and] will limit the scope of application of this decision to data deletion requests that concern features other than Google Search." *Id.* The Italian DPA further required that "the relevant data should be deactivated over the initial 30 days." *Id.* It was further stipulated that "during the period in question the only processing operation allowed in respect of the relevant data shall be the recovering of lost information," while encryption must be used, or "where necessary" anonymization techniques, in order to protect the data against unauthorized access. *Id.*

[138] *See* Natasha Lomas, *Germany Warns Google Over User Profiling Privacy Violations*, TECHCRUNCH (2014), https://techcrunch.com/2014/10/01/hamburg-google/ [https://perma.cc/UG99-33JS]. For example, it may be possible to compile detailed travel profiles by evaluating location data; to detect specific interests and preferences by evaluating search engine use; to assess the user's social and financial status, their whereabouts, and many other of their habits by analyzing the collected data; and to infer information such as friend relationships, sexual orientation and relationship status.

what Google was ordered to do and leaving open the possibility of adding additional requirements at a later date. [139]

[27] What is significant about these actions is that they demonstrate the commitment to data protection in the European Union and help reiterate the WP 29 and EU DPAs' recommendations that under EU data protection law notices must be given for each separate service provided, and that the sharing of information between different services without user consent is prohibited; emphasizing the data retention time limit requirements and the importance of complying with the DPAs' regulations and orders.

c. Google Spain—"Right to Be Forgotten"

[28] The *Google Spain* case involved an action by Mr. Mario Costeja Gonzáles after Google refused to remove a link to a 1998 newspaper article regarding a real estate foreclosure as part of social security debt collection activities against Costeja Gonzales.[140] Costeja Gonzáles argued that the old link contained obsolete information and was prejudicial to him.[141] He

[139] *See* Article 29 Letter Sept. 23, 2014, *supra* note 125. The appendix, which deals with the issues of information requirements (including those for specific services such as YouTube, Google Analytica, and DoubleClick), user controls, and data retention policies, is also available. *See* Article 29 Working Party, *Appendix, List of Possible Compliance Measures*, EUROPEAN COMMISSION, http://webcache.googleusercontent.com/search?q=cache:YgV4u8Khh6cJ:ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy_appendix.pdf+&cd=2&hl=en&ct=clnk&gl=us [https://perma.cc/QK6H-HE85].

[140] *See* James Ball, *Costeja González and a Memorable Fight for the 'Right to be Forgotten'*, THE GUARDIAN (May 14, 2014, 11:34 AM), https://www.theguardian.com/world/blog/2014/may/14/mario-costeja-gonzalez-fight-right-forgotten [https://perma.cc/E7AB-XEAX].

[141] *See* Ashifa Kassam, *Spain's Everyday Internet Warrior Who Cut Free from Google's Tentacles*, THE GUARDIAN, (May 13, 2014, 1:24 PM) https://www.theguardian.om/technology/2014/may/13/spain-everyman-google-mario-costeja-gonzalez [https://perma.cc/FMA3-PD5L?type=image].

brought the case before the Spanish DPA (AEPD), which upheld his complaint against Google Spain SL and Google Inc.[142] Google Spain SL and Google Inc. challenged the AEPD's decision in the Spanish Audencia Nacional (National High Court), which then referred relevant questions about the 95 Directive to the Court of Justice of the European Union (ECJ).[143] The ECJ ruled in Costeja Gonzáles's favor, indicating that an individual's objection to a search engine's link to personal information would require the weighing of the public's interest in the information, the relevance or obsolescence of the information, and the individual's right to keep sensitive data out of the public eye.[144] In response to the court's order, at the end of May 2014 Google set up an online form for exercising the right to delist.[145]

---

[142] *See* W. Gregory Voss, *The Right to be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation*, 18 J. INTERNET L. 3, 3–4 (July 2014) [hereinafter Voss, *The Right to Be Forgotten*].

[143] *See id.*

[144] *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, EUR-LEX, at ¶¶ [81], [88], [99] (2014), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131 [https://perma.cc/C5AF-EXWH]; Stephanie Condon, *Google 'Right to be Forgotten' Case Goes to Top EU Court*, ZDNET (July 19, 2017, 6:05 PM), https://www.zdnet.com/article/google-right-to-be-forgotten-case-goes-to-top-eu-court/ [https://perma.cc/N47D-BNSV. One scholar has noted how the Google Spain case is in direct contravention of U.S. ideology, especially as it concerns the public's right to know and how the EJC's opinion contains logical inconsistencies. *See* Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981, 985–87, 990, 1072 (2018).

[145] *See Google Sets Up 'Right to be Forgotten' Form After EU Ruling*, BBC NEWS (May 30, 2014), http://www.bbc.com/news/technology-27631001 [https://perma.cc/WWU2-BJ5G]. As of September 23, 2018, Google had received 727,095 delisting requests, examined 2,767,505 URLs after delisting requests, and had deleted 1,044,772 (44%) URLs from search results. *See Transparency Report: Search Removals Under European Privacy Law*, GOOGLE, https://transparencyreport.google.com/eu-privacy/overview [https://perma.cc/P2PK-XR6G?type=image]).

[29] In addition, in the fall of 2014 Google set up an advisory council to help it determine when to honor delisting requests and held hearings in major EU capital cities.[146] The advisory council's report suggested that since 95% of Internet searches in Europe used country-specific domains (a figure supplied by Google), that Google would be compliant if it removed the information from the country domain at issue.[147] Google alleged that it had complied with the 2014 ruling by removing the results from the country-code top level domain addresses of the search engines corresponding to the affected countries in Europe (e.g., .de for Germany, .es for Spain, .fr for France, etc.).[148] However, WP 29 indicated that the guidelines in its order required them to remove the information from all searches and all domains (e.g., generic domain .com).[149] On May 15, 2015, the CNIL issued an order for Google to completely remove the information from all of the possible searches and domains.[150] Google replied that "no

[146] *See* Jef Ausloos, *Forget, Erase and Delist, But Don't Forget the Broader Issue*, INTERNET POL'Y REV. (Jan. 22, 2015), https://policyreview.info/articles/news/forget-erase-and-delist-dont-forget-broader-issue/353 [https://perma.cc/783H-DMZA]; *see also Advisory Council to Google on the Right to be Forgotten*, GOOGLE, https://archive.google.com/advisorycouncil/ [https://perma.cc/RN8L-88SD] (discussing the role of the Advisory Council to Google in balancing one person's right to be forgotten and the public's right to information).

[147] *See* Luciano Floridi et al., *The Advisory Council to Google on the Right to be Forgotten*, GOOGLE 19 (Feb. 6, 2015) https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf [https://perma.cc/X952-6TRX].

[148] *See id.* at 18–20; *see also* Condon, *supra* note 144.

[149] *See* Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, 14/EN WP 225, at 3, 9, (Nov. 26, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf [https://perma.cc/59MS-7BBZ].

[150] *See CNIL Orders Google to Apply Delisting on All Domains of the Search Engine*, CNIL (June 12, 2015), https://www.cnil.fr/fr/node/15790 [https://perma.cc/9QKV-FYHV].

one country should have the authority to control what content someone in a second country can access" and that the CNIL did not have global authority to issue such an order.[151] The ECJ has yet to issue its decision on whether or not Google must remove the complained of data from searches worldwide or just in Europe.[152]

2. Facebook

a. Schrems (Safe Harbor case)

[30] This case was brought by Maximillian Schrems, an Austrian citizen, with respect to Facebook's cross-border transfer of data.[153] As a Facebook user, Schrems's personal data was transferred from servers in Ireland to servers in the U.S.[154] The 95 Directive only permitted cross-border transfers if the receiving country ensured an adequate level of protection by reason of domestic law or international agreements.[155] Because the Snowden revelations revealed that U.S. law offered no real protection against surveillance by the U.S. government with respect to data transferred there, Schrems filed an action with the Irish Data Protection Commissioner (DPC).[156] The DPC dismissed Schrems' case indicating that the transfer

[151] Peter Fleischer, *Implementing a European, Not Global, Right to be Forgotten*, GOOGLE EUR. BLOG (July 30, 2015), https://europe.googleblog.com/2015/07/implementing-european-not-global-right.html [https://perma.cc/E4H3-E2J7].

[152] *See, e.g.*, Condon, *supra* note 144 (discussing whether Google must delist certain search results globally).

[153] *See* Case C-362/14, Schrems v. Data Prot. Comm'r, EUR-LEX, at ¶¶ [6], [28] (2015), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN [https://perma.cc/X8H9-8M8X].

[154] *See id.* at ¶¶ [27], [28], [30], [31].

[155] *See id.* at ¶ [96].

[156] *See id.* at ¶¶ [28], [30].

was permitted under the Safe Harbor agreement between the U.S. and Europe.[157] After Schrems appealed, the case was sent to the ECJ which in 2015 invalidated the Safe Harbor agreement that U.S. companies had relied upon in transferring data from Europe to the U.S.[158]

[31] The ECJ found the Safe Harbor agreement invalid because the personal data transferred to the U.S. by Facebook Ireland Ltd to servers belonging to its parent company Facebook Inc. in the U.S., did not receive adequate protection due to "the significant over-reach" of, *inter alia*, the National Security Agency's surveillance.[159] Specifically, the ECJ further ruled that the Safe Harbor Framework was invalid for several reasons: it

[157] *See id.* at ¶¶ [1], [2]. The 95 Directive was intended to provide guidance to the member states and harmonize privacy laws throughout Europe. It required the member states to create laws to protect citizens' information following the terms of the 95 Directive, although each member state could determine how to do that, and provided that personal data could not be transferred to other countries unless those countries had similar protections in place. Because the U.S. was not considered to have these protections, the Safe Harbor was created as discussed above. *See supra* Section II(A)(2). The only other countries that qualified were Andorra, Argentina, Canada (for commercial organizations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay. *See Adequacy of the Protection of Personal Data in Non-EU Countries*, EUR. COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en [https://perma.cc/CX39-CW7U].

[158] *See* Court of Justice of the European Union, Press Release No. 117/15, The Court of Justice Declares that the Commission's US Safe Harbor Decision Is Invalid (Oct. 6, 2016), https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf [https://perma.cc/DS3G-6EUZ].

[159] *See* Case C-362/14 Schrems v. Data Prot. Comm'r, EUR-Lex, at ¶¶ [28]–[30] (2015). According to the NSA, the U.S. Intelligence Community relied on Section 702 of the Foreign Intelligence Surveillance Act to compel providers to facilitate surveillance on specific foreign targets located outside the U.S. for the purpose of acquiring critical intelligence on issues ranging from international terrorism to cybersecurity. *See Expanded Look—"Section 702" Saves Lives, Protects the Nation and Allies*, NSA: CENTRAL SECURITY SERVICE (Dec. 12, 2017), https://www.nsa.gov/news-features/news-stories/2017/702-saves-lives-protects.shtml [https://perma.cc/X96Q-NYMF].

allowed for government interference of the 95 Directive's protections, it did not provide legal remedies for individuals who seek to access data related to them or to have their data erased or amended, and it prevented national supervisory authorities from appropriately exercising their powers.[160]

b. Facebook Cookies Cases—CNIL

[32] In 2013, France published rules confirming that the use of cookies requires the user's consent.[161] It was thereafter discovered that Facebook had been placing cookies on both users' and visitors' browsers without informing them.[162] On May 16, 2017, the CNIL announced that it had fined jointly Facebook Inc. and Facebook Ireland €150,000 for violating the French Data Protection Act, by collecting massive amounts of users' *personal data* and using cookies to obtain behavioral information, without adequately informing the users.[163] The €150,000 fine was the maximum that was allowed under the law at the time the CNIL's investigation began in 2014.[164]

[160] *See* Case C-362/14, Schrems v. Data Prot. Comm'r, EUR-Lex, at ¶ [66] (2015).

[161] *See CNIL Starts Controlling Cookie Settings in October 2014*, IUBENDA, https://www.iubenda.com/blog/cnil-starts-controlling-cookie-settings-october-2014/ [https://perma.cc/Y4XT-ZYXV].

[162] *See Facebook Sanctioned for Several Breaches of the French Data Protection Act*, CNIL (May 16, 2017), https://www.cnil.fr/en/facebook-sanctioned-several-breaches-french-data-protection-act [https://perma.cc/G35C-3B2U].

[163] *Id.*

[164] *See* Loi 2016-1321 du 7 octobre 2016 pour une République numérique [Law no. 2016-1321 of 7 October 2016 For A Digital Republic], Journal Officiel de la République Française [J.O.] [Official Journal of the French Republic], Oct. 8, 2016, 14 (as a result of an amendment made by France's Digital Republic Act, the French Data Protection Act later authorized fines for data protection violations of up to €3 million); Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties] Jan. 7, 1978.

[33] The Contact Group of the Data Protection Authorities of the European Union (Contact Group),[165] which was formed in 2014 to address this issue, asserted that their respective national data protection laws do apply to the processing of personal data of users and non-users by Facebook,[166] consistent with case law from the European Court of Justice (the cases of *Google Spain*, *Weltimmo* and *Amazon*)[167] and Article 4(1)(a) of the 95 Directive.[168] Facebook, however, disputed their authority.[169] The DPAs pointed to the presence of multiple Facebook offices in the European Union and their targeted advertising to users and non-users in the EU.[170]

[34] Investigations were also conducted by Belgium, the Netherlands, Germany and Spain for data privacy violations around the tracking of users and non-users and the use of user data for targeted advertising.[171] In February 2018, a Belgian court ordered Facebook to stop breaking privacy laws by tracking people on third-party websites or risk a fine of €250,000 a day, up to €125 million, if it did not comply with the court's judgment,

[165] *See* Common Statement by the Contract Group of the Data Protection Authorities of the Netherlands, France, Spain, Hamburg, and Belgium (May 16, 2017) [hereinafter Common Statement] (The Contract Group consists of the DPAs from the Netherlands, France, Spain, Hamburg (on behalf of Germany) and Belgium).

[166] *See id.*

[167] *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ¶¶ [1]–[4] (2014); *see also* Case C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmiés Információszabadság Hatóság ¶ [66] (2015); Case C-191/15, Verein für Konsumenteninformation v. Amazon EU Sàrl, ¶ [82] (2016); Ward & Van den Bulck, *supra* note 108.

[168] 95 Directive, *supra* note 13, at art. 4(1)(a).

[169] *See* Samuel Gibbs, *Facebook Facing Privacy Actions Across Europe as France Fines Firm €150k*, THE GUARDIAN (May 16, 2017, 11:23 AM), https://www.theguardian.com/technology/2017/may/16/facebook-facing-privacy-actions-across-europe-as-france-fines-firm-150k [https://perma.cc/QW8C-SYEX].

[170] *See* Common Statement, *supra* note 165.

[171] *See generally id.*

which Facebook is reported to be appealing.[172] In September 2017, the Spanish DPA fined Facebook a total of €3 million for its violations.[173] In May 2017, the Dutch DPA concluded that Facebook had violated privacy law and the DPA reserved the right to impose sanctions later.[174] In February 2018, the German regional court in Berlin ruled that Facebook failed to provide enough information to users to obtain informed consent and that Facebook's pre-checked opt-in boxes violated German privacy and data protection law.[175]

[35] The violations related to the "quality of the information provided to users, the validity of consent and the processing of personal data for advertising purposes."[176] The French authorities indicated that Facebook was using cookies to collect browsing data of Internet users without their knowledge or consent. [177] Facebook has argued that they are only subject to the privacy and data protection laws of Ireland where their European

[172] *See* Robert-Jan Bartunek, *Facebook Loses Belgian Privacy Case, Faces Fine of up to $125 Million*, REUTERS (Feb. 16, 2018, 10:00 AM), https://www.reuters.com/article/us-facebook-belgium/facebook-loses-belgian-privacy-case-faces-fine-of-up-to-125-million-idUSKCN1G01LG [https://perma.cc/G9UQ-NQ2V].

[173] *See* Robert Hetz & Isla Binnie, *Facebook Fined 1.2 Million Euros by Spanish Data Watchdog*, REUTERS (Sept. 11, 2017, 9:26 AM), http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_09_11-iden-idphp.php [https://perma.cc/AWF7-VBFN].

[174] *See Dutch Data Protection Authority: Facebook Violates Privacy Law*, AUTORITEIT PERSOONSGEGEVENS (May 16, 2017), https://autoriteitpersoonsgegevens.nl/en/news/dutch-data-protection-authority-facebook-violates-privacy-law [https://perma.cc/4TH9-WHCT].

[175] *See* Akira Tomlinson, *Germany Court Rules Facebook Personal Data Usage Illegal*, JURIST (Feb. 12, 2018, 1:13 PM), https://www.jurist.org/news/2018/02/germany-court-rules-facebook-personal-data-usage-illegal/ [https://perma.cc/2SDJ-3XVD].

[176] *See* Common Statement, *supra* note 165.

[177] *See* Gibbs, *supra* note 169.

subsidiary is located.[178] The ECJ ruled to the contrary, however, in *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*.[179] A company (in this case, Facebook) may be subject to the data protection law of the country where they have an establishment (in this case, Germany), even when the responsibility for data collecting and processing for all the European Union is held by a sister company in another EU member state (in this case, Ireland):

> where an undertaking established outside the European Union has several establishments in different Member States, the supervisory authority of a Member State is entitled to exercise the powers conferred on it by Article 28(3) of [the 95 Directive] with respect to an establishment of that undertaking situated in the territory of that Member State even if, as a result of the division of tasks within the group, first, that establishment is responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State and, second, exclusive responsibility for collecting and processing personal data belongs, for the entire territory of the European Union, to an establishment situated in another Member State.[180]

B. U.S. Data Privacy Law Enforcement Actions

[36] Although U.S. actions against U.S. tech companies have been relatively rare,[181] this section will compare U.S. enforcement activities

[178] *See id.*

[179] See Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH (2018).

[180] See *id.*, at ¶ [64].

[181] *See generally FTC: Investigating Google Street View Is a "Waste of Summer,"* ELECTRONIC PRIVACY INFO. CTR. (Jan. 20, 2011) [hereinafter *FTC Investigating Google*], https://epic.org/2011/01/ftc-investigating-google-stree.html [https://perma.cc/598L-

resulting from the same or similar activities which gave rise to the European DPA actions.

1. Google

a. Google Street View

[37] In May 2010, after Congress became aware of European regulators' investigation of Google's Street View, it asked the FTC to investigate.[182] In 2011, the FTC dropped its investigation into Google Street View, even as countries in the EU were assessing fines against Google for violating their privacy laws, because Google assured the FTC that it had stopped this practice.[183] According to the FTC:

> To this end, we note that Google has recently announced improvements to its internal processes to address some of the concerns raised above, including appointing a director of privacy for engineering and product management; adding core privacy training for key employees; and incorporating a formal privacy review process into the design phases of new initiatives. The company also publicly stated its intention to delete the inadvertently collected payload data as soon as possible. Further, Google has made assurances to the FTC that the company has not used and will not use any of the payload data collected in any Google product or service, now or in the future. This assurance is critical to mitigate the potential harm to consumers from the collection

DRUU] (stating that U.S. authorities did not open an investigation on Google until EPIC filed a complaint, even after several other countries had already conducted their own investigations).

[182] *See EPIC v. FTC (Google Street View)*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/streetview/foia_1/default.html [https://perma.cc/CX5W-C4JT].

[183] *See FTC: Investigating Google*, *supra* note 181.

> of payload data. Because of these commitments, we are ending our inquiry into this matter at this time.[184]

[38] Around the same time, the Federal Communications Commission (FCC) opened an investigation into Google's Street View activities after the Electronic Privacy Information Center (EPIC) filed a complaint, asking the FCC to investigate violations of Section 705 of the Communications Act which adds additional restrictions to the Federal Wiretap Act prohibiting the unauthorized interception of communication "by wire or radio."[185] Section 705 requires establishing both the interception and use of a communication, whereas the Wiretap Act is violated by interception alone.[186] Although the FCC fined Google $25,000 for obstructing its investigation, it never made a final determination that the collection of wi-fi data violated federal law.[187] Google was not required to turn over the intercepted data, alleging it to be a trade secret and the key witness asserted his Fifth Amendment right against self-incrimination.[188] Thus, no action was ever taken to hold Google accountable for its Street View activities in the U.S., contrary to findings that such activities violated European law.[189]

---

[184] Letter from David C. Vladeck, Fed. Trade Comm'n, to Albert Gidari, Esq., Counsel to Google (Oct. 27, 2010), https://www.ftc.gov/sites/default/files/documents/closing_letters/google-inquiry/101027googleletter.pdf [https://perma.cc/L24T-CES6].

[185] *See* 47 U.S.C. § 605 (2018).

[186] *See* 18 U.S.C. § 2511 (2018).

[187] *See* Charles Arthur, *Google fined by FCC over Street View*, THE GUARDIAN (Apr. 16, 2012 3:05 PM), https://www.theguardian.com/technology/2012/apr/16/google-fined-fcc-street-view [https://perma.cc/V3HM-Q45Y].

[188] *See id.*

[189] *See id.*

b. Google Buzz/Safari

[39] In 2010, Google launched the social media platform Google Buzz which allowed users to share information via posts which could be deemed public or private.[190] Google then prepopulated the platform with users' email addresses and names, as well as the names and email addresses of their contacts.[191] This was considered to be an unfair practice by the FTC because Google had previously represented in its Gmail privacy policy that the information provided to create a Gmail account would only be used for email.[192] In addition, the posts were made public by default contrary to its privacy policy which indicated that Google would seek a user's consent prior to using their information for a purpose other than for which it was initially collected.[193] Like most consent decrees, Google agreed that it

[190] *See* Press Release, Fed. Trade Comm'n, FTC Charged Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network (Mar. 30, 2011) [hereinafter FTC March 30, 2011 Press Release] https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz [https://perma.cc/K3PU-8WYA].

[191] *See* Google, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 76 Fed. Reg. 18762, 18763 (proposed Apr. 5, 2011).

[192] *See id.*

[193] *See id.* ("Part I of the proposed order prohibits Google from misrepresenting the privacy and confidentiality of any 'covered information,' as well as the company's compliance with any privacy, security, or other compliance program, including but not limited to the U.S.-EU Safe Harbor Framework [. . .] Part II of the proposed order requires Google to give Google users a clear and prominent notice and to obtain express affirmative consent prior to sharing the Google user's information with any third party in connection with a change, addition or enhancement to any product or service, where such sharing is contrary to stated sharing practices in effect at the time the Google user's information was collected [. . .] Part III of the proposed order requires Google to establish and maintain a comprehensive privacy program that is reasonably designed to: (1) Address privacy risks related to the development and management of new and existing products and services, and (2) protect the privacy and confidentiality of covered information. The privacy program must be documented in writing and must contain privacy controls and procedures appropriate to Google's size and complexity, the nature and scope of its activities, and the sensitivity of covered information [. . .] Part IV of the proposed order requires that Google obtain within 180 days, and on a biennial basis

would not do this again.[194] But in 2012, Google agreed to pay a $22.5 million fine to the FTC for violating the consent decree by representing to users of Apple's Safari that it would not place cookies on searches or use them for targeted advertisements when it in fact did.[195]

c. Google Privacy Policy

[40] In 2012, Google's changes to its privacy policy (allowing Google to combine personal information from one of its services with another), which resulted in a fine by the CNIL and others as mentioned above, also instigated a complaint by EPIC in the DC District Court. EPIC demanded that the FTC enforce its consent decree with Google which required Google to expressly permit users to opt out prior to Google sharing information with third parties.[196] The court dismissed the complaint by EPIC indicating that the FTC had discretion over which actions to bring.[197] When Google tried to change its privacy policy in 2016 permitting the combination of DoubleClick's data with its own, Consumer Watchdog filed a complaint

---

thereafter for twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: it has in place a privacy program that provides protections that meet or exceed the protections required by Part III of the proposed order; and its privacy controls are operating with sufficient effectiveness to provide reasonable assurance that the privacy of covered information is protected.").

[194] *See* FTC March 30, 2011 Press Release, *supra* note 190.

[195] *See* Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser, (Aug. 9. 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented [https://perma.cc/4ALR-SARB].

[196] *See* Casey Johnston, *Privacy Group Demands FTC Force Google to Roll Back Privacy Policy Changes*, ARS TECHNICA (Feb. 9, 2012, 12:44 PM), https://arstechnica.com/gadgets/2012/02/privacy-group-demands-ftc-force-google-to-roll-back-privacy-policy-changes/ [https://perma.cc/5PDF-EJ4A].

[197] *See* Elec. Privacy Info. Ctr. v. FTC, 844 F. Supp. 2d 98, 106 (D.D.C. 2012).

with the FTC asking it to investigate the change.[198] The change was promoted to the public as giving users greater control over their data, but Google failed to expressly inform the users that it would be combining user's personally identifiable information (PII) with advertiser's browsing data.[199] In August, 2017, EPIC filed a complaint with the FTC against Google for using credit card information to evaluate the success of ads without giving consumers a reasonable way to opt out of the collection and use of their information.[200] There has been no investigation or resolution by the FTC as of this time.[201]

2. Facebook

a. Facebook Privacy Policy

[41] In 2011 the FTC brought an action against Facebook because of changes it made to its website, which contradicted what it told to its users.[202]

---

[198] *See* Complaint at 1, *In re* Google Inc.'s Change in Data Use Policies, (F.T.C. Dec. 16, 2016), http://www.consumerwatchdog.org/resources/ftc_google_complaint_12-5-2016docx.pdf [https://perma.cc/X5KL-26EY].

[199] *See* Cynthia J. Larose & Michael B. Katz, *2017 Federal Trade Commission and Google Complaint*, NAT'L L. REV. (Jan. 4, 2017), https://www.natlawreview.com/article/2017-federal-trade-commission-and-google-complaint [https://perma.cc/2Q7G-72T6].

[200] *See* George Lynch, *Privacy Group FTC Privacy Petition Challenges Google Ad Program*, BLOOMBERG NEWS (Aug. 1, 2017), https://www.bna.com/privacy-group-ftc-n73014462591/ [https://perma.cc/4G8Y-ARXN]; *see also,* Complaint, at 1, *In re* Google, Inc. (F.T.C. July 31, 2017), https://epic.org/privacy/ftc/google/EPIC-FTC-Google-Purchase-Tracking-Complaint.pdf [https://perma.cc/CC8G-9UVN].

[201] *See* Letter from Marc Rotenberg, EPIC President and Sam Lester, EPIC Consumer Privacy Counsel to Joseph Simons, Chairman, FTC (May 7, 2018), https://epic.org/privacy/google/purchase-tracking/EPIC-FTC-Google-Tracking-05-2018.pdf [https://perma.cc/S7F3-JXV2].

[202] *See* Press Release, Fed. Trade Comm'n., Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises, FTC (Nov. 29, 2011),

Although users could choose in their privacy setting that their data would be shared with "Only Friends," it was in fact shared with third parties.[203] Although Facebook denied this, the FTC alleged and included in its consent decree that advertisers had been made privy to personally identifiable information of Facebook users when they clicked on an ad in their feed.[204] In addition, the complaint alleged that information could be accessed by Facebook even after a user deleted their account.[205] The FTC also concluded that Facebook did not comply with the US-EU Safe Harbor agreement despite certifying that it did.[206]

---

https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep [https://perma.cc/5FE6-VGQB].

[203] *See id.*

[204] *See id.*

[205] *See id.*

[206] "The FTC complaint lists a number of instances in which Facebook allegedly made promises that it did not keep:

- In December 2009, Facebook changed its website so certain information that users may have designated as private—such as their Friends List—was made public. They didn't warn users that this change was coming, or get their approval in advance.
- Facebook represented that third-party apps that users' installed would have access only to user information that they needed to operate. In fact, the apps could access nearly all of users' personal data—data the apps didn't need.
- Facebook told users they could restrict sharing of data to limited audiences—for example with "Friends Only." In fact, selecting "Friends Only" did not prevent their information from being shared with third-party applications their friends used.
- Facebook had a "Verified Apps" program & claimed it certified the security of participating apps. It didn't.
- Facebook promised users that it would not share their personal information with advertisers. It did.
- Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible. But Facebook allowed access to the content, even after users had deactivated or deleted their accounts.
- Facebook claimed that it complied with the U.S.- EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union. It didn't."

[42] On August 10, 2012, the FTC entered into a consent decree with Facebook regarding the charges that Facebook deceived consumers by telling them their information on Facebook was private and then allowing it to be shared and made public.[207] "The settlement requires Facebook to take several steps to make sure it lives up to its promises in the future, including by giving consumers clear and prominent notice and obtaining their express consent before sharing their information beyond their privacy settings, by maintaining a comprehensive privacy program to protect consumers' information, and by obtaining biennial privacy audits from an independent third party." [208] In August 2016, EPIC filed a complaint against Facebook with the FTC for transferring previously collected WhatsApp user data to Facebook for targeted advertising purposes.[209] This was alleged to be an unfair and deceptive trade practice because at the time Whatsapp collected the data, the privacy policy did not mention that it could be transferred to Facebook.[210] FTC has not made a ruling as of this time, although they have indicated that they are reopening the investigation into Facebook's privacy practices.[211]

See id.

[207] *See* FTC August 10, 2012 Press Release, *supra* note 10.

[208] *Id.*

[209] *See* In re WhatsApp, ELECTRONIC PRIVACY INFO. CTR., [hereinafter EPIC, *In re WhatsApp*] https://epic.org/privacy/internet/ftc/whatsapp/#Acquisition [https://perma.cc/TF93-728N].

[210] *See* Complaint, at 1, *In re* WhatsApp, Inc., (F.T.C. Aug. 29, 2016), https://www.democraticmedia.org/sites/default/files/field/public/2016/epic-cdd-ftc-whatsapp-complaint-2016.pdf [https://perma.cc/7YCU-DF5L].

[211] *See* EPIC, *In re WhatsApp*, (October 15, 2018), *https://www.epic.org/privacy/internet/ftc/whatsapp/* [https://perma.cc/R3CL-N75P] (citing FTC, Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices, (March 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection [https://perma.cc/B69C-5XKZ]).

[43] More recently, the FTC is investigating Facebook's handling of user information in light of the Cambridge Analytica's access to the data of 50–90 million Facebook users which may have impacted the last presidential election.[212] Mark Zuckerberg testified in front of 44 members of the Senate the week of April 10, 2018.[213] The last time Zuckerberg was pulled in front of the committee was in October 2017 to answer questions about how Facebook may have been involved in the spreading of fake news prior to the election.[214]

C. Differences Between EU and U.S. Enforcement Actions

[44] What is most telling about the FTC enforcement actions is that besides fines and promises made by Google and Facebook, there appears to have been no further monitoring of their actions, contrary to the consent decrees that require annual audits to ensure compliance with the orders.[215] Although EPIC continues to bring suits attempting to force the FTC to enforce these settlement decrees, the courts have consistently held that

[212] *See* Tiffany Hsu & Ceclia Kang, *Demands Grow for Facebook to Explain Its Privacy Policies*, N.Y. TIMES (Mar. 26, 2018), https://nyti.ms/2pIJY12 [https//perma.cc./X7HC-BEN5]; *see also* Complaint, at 1, *In re* WhatsApp, Inc., (F.T.C. Aug. 29, 2016), https://www.democraticmedia.org/sites/default/files/field/public/2016/epic-cdd-ftc-whatsapp-complaint-2016.pdf [https://perma.cc/7YCU-DF5L].

[213] *See* Bloomberg Government, *Transcript of Mark Zuckerber'g Senate Hearing*, WASHINGTON POST (Apr. 10, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.ac0dcdb56eff [https://perma.cc/S744-QN2Q].

[214] *See* Austin Carr, *Senators Grill Facebook, Twitter & Google On Fake News: "Your Power Scares Me,"* FAST COMPANY (Oct. 31, 2017), https://www.fastcompany.com/40489793/senators-grill-facebook-twitter-google-on-fake-news-your-power-scares-me [https://perma.cc/5QHG-ELRP].

[215] *See* Kirk Victor, *FTC Failed to Enforce Facebook Consent Decree, Critics Charge Amid Firestorm*, MLEX (Apr. 2, 2018), https://mlexmarketinsight.com/contact-us/ftcwatch/selected-2017-articles/ftc-failed-to-enforce-facebook-consent-decree,-critics-charge-amid-firestorm [https://perma.cc/QV29-W22J].

EPIC cannot force a discretionary agency action.[216] In addition, the FTC seems hesitant to insert itself into these companies' affairs.[217] For example, Price Waterhouse Coopers was retained by the FTC to audit Facebook's privacy practices to ensure compliance with its 2011 consent decree.[218] The audit, provided to EPIC pursuant to a FOIA request, indicated that "Facebook's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy" of covered information through February 2017.[219] The audit was conducted after a significant amount of profile data was provided to Cambridge Analytica.[220] The FTC released only portions of the audit claiming the trade secret exemption to FOIA.[221] According to Marc Rotenberg, Executive Director of EPIC, "It's troubling [. . .] that the FTC seems unwilling to bring any legal action against either Facebook or Google to enforce privacy settlements."[222]

[45] From the EU enforcement actions that we have reviewed above, several lessons may be gleaned for compliance under EU data protection regulation. First, we have seen that EU data protection law has

[216] *See id.*

[217] *See id.*

[218] Nicholas Confessore, *Audit Approved of Facebook Policies, Even After Cambridge Analytica Leak*, N.Y. TIMES (Apr. 19, 2018), https://www.nytimes.com/2018/04/19/technology/facebook-audit-cambridge-analytica.html [https://perma.cc/CKQ9-KKCP].

[219] *See id.*

[220] *See id.*

[221] *See id.*

[222] Thomas Claburn, *Facebook Privacy Audit by Auditors Finds Everything is Awesome!*, THE REGISTER (Apr. 21, 2018, 12:09 AM), https://www.theregister.co.uk/2018/04/21/facebook_privacy_audit_finds_everything_is_awesome/ [https://perma.cc/R696-H795].

extraterritorial effect,[223] a subject we will be addressing further in the context of the GDPR in Section IV below. The jurisdiction of the EU member state DPAs may extend to U.S. technology companies,[224] and thus the latter must take this into consideration in their compliance efforts. Secondly, the Google Street View cases have pointed out the importance of incorporating *privacy by default and design* from the start to prevent violations, a concept discussed further below.[225] This is especially important in the context of future potential fines and EU member state DPAs' powers under the GDPR. We have seen one example where good privacy-enhancing design by Google could have avoided the problems that its Street View service encountered.[226] In effect, Google failed to take into account harms their street collection actions could have caused.[227] In addition, these cases highlight the importance of understanding the broad definition of *personal data* under EU legislation, and the necessity of taking that into consideration when devising compliance programs and designing new products and services.

[46] Next, the Google Privacy Policy actions underscored the importance of engaging the relevant EU member state DPAs prior to taking any action,

[223] *See* Lucy Handley, *US Companies Are Not Exempt from Europe's New Data Privacy Rules—And Here's What They Need to Do About It*, CNBC (APR. 25, 2018, 11:10 AM), https://www.cnbc.com/2018/04/25/gdpr-data-privacy-rules-in-europe-and-how-they-apply-to-us-companies.html [https://perma.cc/AC2M-Z74U].

[224] *See id*.

[225] *See* Shay Danon, *GDPR Top Ten #6: Privacy by Design and by Default*, DELOITTE, https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-privacy-by-design-and-by-default.html# [https://perma.cc/4YJ3-PNMV].

[226] *See* David Kravets, *An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle*, WIRED (May 2, 2012, 7:18 PM), https://www.wired.com/2012/05/google-wifi-fcc-investigation/ [https://perma.cc/M8GT-DA9L].

[227] *See id.* (indicating that there is a conflict as to whether Google intended to collect wi-fi data or whether it was a bug in its software).

such as instituting a new user policy.[228] In that case, Google had presented the DPAs with more or less a *fait accompli*, which led to problems.[229] Furthermore, respect of EU data protection principles based originally on OECD guidelines, such as requirements of transparency (including providing information or notice to the data subject as to processing of personal data), was shown to be crucial.[230] Other lessons from these cases include the necessity of complying with the purpose limitation (with the necessary definition of the purpose of collection and processing), and the limiting of the time period for retention of data so that data is not kept indefinitely.[231] In addition, the importance of initiating procedures to comply with requests for the exercise of data subject rights, such as responding to data deletion requests, was made evident in the *Google Spain* case.[232] There, Google was forced to rapidly institute procedures after the ECJ decision, establishing an online link-deletion request form.[233] Moreover, as was seen in the Facebook Privacy case, adequate information

[228] *See* Katie Collins, *Google Makes Privacy Policy Clearer Than Ever to Comply with EU Law*, CNET (May 11, 2018, 5:00 AM), https://www.cnet.com/news/google-makes-privacy-policy-clearer-than-ever-to-comply-with-eu-gdpr-law/ [https://perma.cc/3VGU-9DEN].

[229] *See* Chris Ciaccia, *Facebook and Google Slammed, Accused of Breaking New GDPR Data Privacy Law* FOX NEWS (May 25, 2018) http://www.foxnews.com/tech/2018/05/25/facebook-and-google-slammed-accused-breaking-new-gdpr-data-privacy-law.html [https://perma.cc/M3JK-MYJ7].

[230] *See How Did We Get Here? An Overview of Important Regulatory Events Leading Up to the GDPR*, EU GDPR.ORG, https://eugdpr.org/the-process/how-did-we-get-here/ [https://perma.cc/VG3C-XU36].

[231] *See Principle (b): Purpose Limitation*, ICO, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ [https://perma.cc/94LZ-SP5K].

[232] *See* Case C-131/12, Google Spain SL v. Agencia Española de Proteccíon de Datos (2014).

[233] *See* Richard Trenholm, *You Can Now Ask Google to Remove Links About You*, CNET (May 30, 2014, 2:51 AM), https://www.cnet.com/news/you-can-now-ask-google-to-remove-links-about-you/ (last visited Oct. 28, 2018).

must be provided to the user and his or her consent should be obtained before placing a cookie on a user's device.[234]

[47] The *Google Spain* "right to be forgotten" case served to extend an existing right, which does not exist in the United States—the right to deletion and/or correction of personal data when inaccurate or obsolete. The right requires the delisting of links to such data on the Internet by search engines, when requested by data subjects, after a balancing of the interests of the public to such information with the privacy rights of the relevant data subject.[235] Furthermore, the French DPA maintained that such delisting must be applied to Internet domains worldwide, not just EU domains.[236]

[48] The Facebook cross-border data transfer case involving the invalidation of the Safe Harbor was very enlightening in many respects. First, it demonstrated that a data subject has the right to access his or her personal data held by the technology company, as Schrems exercised this right to obtain his data from Facebook.[237] Second, the case showed the impact of U.S. mass surveillance on arrangements between the EU and the U.S. as discussed above in Section III(A)(2)(a) and as evidenced in the Privacy Shield negotiations.[238] Finally, the ECJ's decision highlighted the

[234] This general concept of prior informed consent was enshrined in the ePrivacy Directive (Directive 2002/58/EC) by the 2009 amendments to it (Directive 2009/136/EC), and this is expected to be modified by a proposed ePrivacy Regulation. *See* W. Gregory Voss, *First the GDPR, Now the Proposed ePrivacy Regulation*, 21 J. INTERNET L. 3, 5–6 (2017).

[235] *See generally* Case C-131/12, Google Spain v. Agencia Española de Proteccíon de Datos (2014).

[236] *See* Alex Hern, *Google Says Non to French Demand to Expand Right to be Forgotten Worldwide* (Jul. 30, 2015, 12:00 PM), https://www.theguardian.com/technology/2015/jul/30/google-rejects-france-expand-right-to-be-forgotten-worldwide [https://perma.cc/KU4B-W5AY].

[237] *See* Lee Matheson, *Understanding 'Schrems 2.0'*, IAPP: THE PRIVACY ADVISOR, https://iapp.org/news/a/understanding-schrems-2-0/ [https://perma.cc/8JW9-A2NB].

[238] *See infra* Section IV(D).

importance attributed to data protection as a fundamental right of individuals in EU courts.[239] Companies relying on the Privacy Shield should bear this in mind.

[49] However, with respect to anticipated actions, it is very likely that, because of the wide Cambridge Analytica publicity, the FTC will be taking some sort of action against Facebook.[240] Christopher Wylie, who previously worked at Cambridge Analytica, was one of the designers involved in using data from Facebook to create psychological profiles of votes both within the U.S. and Britain.[241] These profiles were then used to target political ads which are alleged to have influenced both the U.S. presidential election and the Brexit vote.[242] Although Cambridge Analytica has been the subject of investigations in both countries (Robert Mueller's in the US, and the Electoral Commission and the Information Commissioner's Office in the UK), both triggered in February 2017, due to an Observer article, the extent

[239] *See* Courtney Bowman, *US-EU Safe Harbor Invalidated: What Now?*, PROSKAUER: PRIVACY LAW BLOG (Oct. 6, 2015), https://privacylaw.proskauer.com/2015/10/articles/european-union/us-eu-safe-harbor-invalidated-what-now/ [https://perma.cc/C6XP-GSZ5].

[240] It is not possible, however, to anticipate the result of such an investigation as Facebook has already argued that it complied with the 2011 consent decree. It does seem that it stopped Cambridge Analytica's access once the breach was discovered but did not notify the FTC. This will most likely be the primary issue.

[241] *See* Carole Cadwalladr, '*I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower*, THE GUARDIAN (Mar. 18, 2018, 5:44 AM), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

[242] *See* Patrick Greenfield, *The Cambridge Analytica Files: The Story So Far*, THE GUARDIAN (Mar. 25, 2018, 7:53 PM), https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far [https://perma.cc/KK2V-8SH9]; *see also* Ellen Bary *Cambridge Analytica Whistle-Blower Contends Data-Mining Swung Brexit Vote*, N. Y. TIMES (Mar. 27, 2018), https://www.nytimes.com/2018/03/27/world/europe/whistle-blower-data-mining-cambridge-analytica.html [https://perma.cc/2ZFD-VYFX].

of Facebook's knowledge and involvement is just now being questioned.[243] The focus will be on whether Facebook violated the FTC 2011 consent decree.[244]

[50] However, European legislators are also interested in this affair. Facebook's CTO Mike Schroepfer, whose testimony before a UK parliamentary committee on April 26, 2018 was primarily on fake news, faced tough questioning about Cambridge Analytica.[245] Facebook appeared before the European Parliament on May 22, 2018, just before the GDPR was to apply, however its CEO was generally evasive.[246] According to an earlier article in *The New York Times*, Cambridge Analytica collected data on

---

[243] *See* Craig Timberg et al., *Facebook's Disclosures Under Scrutiny as Federal Agencies Join Probe of Tech Giant's Role in Sharing Data With Cambridge Analytica*, WASHINGTON POST (Jul. 2, 2018), https://www.washingtonpost.com/technology/2018/07/02/federal-investigators-broaden-focus-facebooks-role-sharing-data-with-cambridge-analytica-examining-statements-tech-giant/?utm_term=.04c5b3ae7132 [https://perma.cc/38KJ-945M].

[244] *See* Mariella Moon, *FTC-Mandated Audit Cleared Facebook's Privacy Policies in 2017*, ENGADGET (Apr. 20, 2018), https://www.engadget.com/2018/04/20/ftc-audit-cleared-facebook [https://perma.cc/H7PC-B6U7] ("When asked why Facebook didn't disclose the Cambridge Analytica issue to the external company that did the audit, [Facebook] pointed us to an exchange between US Representative Bob Latte and Mark Zuckerberg during the House hearing, wherein the Facebook chief responded: '[O]ur view is that this—what a developer did—that they represented to us that they were going to use the data in a certain way, and then, in their own systems, went out and sold it—we do not believe is a violation of the consent decree.' Facebook Deputy Chief Privacy Officer Rob Sherman also said in a statement: 'We remain strongly committed to protecting people's information. We appreciate the opportunity to answer questions the FTC may have.'").

[245] *See* Adam Satariano, *Facebook Faces Tough Questions in Britain That It Avoided in the U.S.*, N.Y. TIMES (Apr. 26, 2018), https://nyti.ms/2KjmAjt [https://perma.cc/8C6G-GRNT].

[246] *See* Adam Satariano & Milan Schreuer, *Facebook's Mark Zuckerberg Gets an Earful From the E.U.*, N.Y. TIMES (May 22, 2018), https://nyti.ms/2GDod8J [https://perma.cc/F9T6-L7ZK].

> users' identities, friend networks and "likes." The idea was to map personality traits based on what people had liked on Facebook, and then use that information to target audiences with digital ads. Researchers in 2014 asked users to take a personality survey and download an app, which scraped some private information from their profiles and those of their friends, activity that Facebook permitted at the time and has since banned. The technique had been developed at Cambridge University. . . Dr. Kogan [a professor at Cambridge] built his own app and in June 2014 began harvesting data for Cambridge Analytica.[247]

[51] A hearing will be necessary because there is some dispute as to whether this was a data breach or if the data was given to Cambridge Analytica for academic research.[248] The 95 Directive does not include a provision on data breach notification,[249] but this is a new requirement under the GDPR.[250] Many member states, however, will likely find this to be a violation of their data protection regulations because, regardless of how Cambridge Analytica came to possess this data from Facebook, Facebook

[247] Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/F964-GQ5B].

[248] *See Cambridge Analytica And Facebook: The Scandal So Far*, AL JAZEERA (Mar. 28, 2018), https://www.aljazeera.com/news/2018/03/cambridge-analytica-facebook-scandal-180327172353667.html [https://perma.cc/V2MG-DXAA].

[249] *See* Trevor Williams, *GDPR is Coming: If You're Selling to EU Citizens, Here's How to Be Prepared*, GLOBAL ATLANTA (May 11, 2018), https://www.globalatlanta.com/gdpr-is-coming-if-youre-selling-to-eu-citizens-heres-how-to-be-prepared/ [https://perma.cc/3FZD-AB9P].

[250] *See id.* It should be kept in mind that, as the Cambridge Analytica affair occurred prior to the application of the GDPR, it is member state implementing legislation of the 95 Directive that would apply, instead.

did not gain consent for this use.[251] The UK is especially interested in this issue as it could cast doubt on the legitimacy of the Brexit vote which was already unpopular.[252]

[52] The EU has a robust set of privacy and data security laws which were strengthened with the applicability of the GDPR on May 25, 2018. While there have been hundreds of enforcement actions taken against U.S. tech companies in recent years,[253] the low maximum fines permitted under the laws created pursuant to the 95 Directive have not been substantial enough to force change in the way these tech companies collect and utilize data. This will change with the extraterritorial jurisdiction and enormous fines possible under the GDPR. The FTC is the main agency concerned with privacy and data security in the U.S., but its actions against U.S. tech companies have been few and far between.[254] The penalties imposed in the few actions taken are also not significant enough to force change.[255] While EU actions are public, the FTC investigations and mandatory audits of

[251] *See* Michael Kaplan, *Facebook And Google Are Already Facing Lawsuits Under New Data Rules*, CNN (May 25, 2018, 4:24 AM), https://money.cnn.com/2018/05/25/technology/gdpr-compliance-facebook-google/index.html [https://perma.cc/RW6X-652H].

[252] *See* Mark Scott, *Cambridge Analytica Helped 'Cheat' Brexit Vote and US Election, Claims Whistleblower*, POLITICO (Mar. 27, 2018, 5:46 PM), https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/ [https://perma.cc/PE8B-PGXP].

[253] *See* Jeff John Roberts, *Why Google, Facebook, and Amazon Should Worry About Europe*, FORTUNE (Jul. 20, 2017), http://fortune.com/2017/07/20/google-facebook-apple-europe-regulations/ [https://perma.cc/DD74-7LQS] (explaining that in addition to violations of privacy and data protection law, member states in the EU have brought actions against U.S. tech companies for anti-trust, labor, national security, and tax law violations).

[254] *See* Harper Neigid, *FTC Plans to Reexamine How It Polices Tech Companies*, THE HILL (Jun. 20, 2018, 1:21 PM), https://thehill.com/policy/technology/393270-the-ftc-plans-to-re-examine-how-it-polices-tech-companies [https://perma.cc/9JT7-QKZB].

[255] *See* Kaminski, *supra* note 32, at 948.

Facebook and Google are kept private.[256] Without an overarching federal privacy and data security law, the U.S. relies on state action and the limited power of the FTC to protect consumers from deceptive and unfair practices.

IV. GENERAL DATA PROTECTION REGULATION

[53] In 2012, the European Commission formally initiated the updating of the 95 Directive which had provided the basis for EU member states' local data privacy laws.[257] Although quite advanced when implemented in 1995, further advances in technology and certain shortcomings of the 95 Directive led to the proposal of a new regulation.[258] The proposal was designed to harmonize data protection laws throughout Europe, enhance data transfer rules outside of the EU, and to provide greater control over one's personal data.[259] After several years of discussions, the European Parliament approved the GDPR on April 14, 2016.[260] The main changes that are of concern to American companies are the extraterritorial application, significantly increased administrative sanctions, additional rights provided to data subjects, data breach notification requirements, limitations on profiling, and the introduction of compliance mechanisms (including

[256] *See* Hans, *supra* note 5, at 191.

[257] *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, at 1, 2, COM (2012) 11 final (Jan. 1, 2012) [hereinafter *Proposal for a Regulation*].

[258] *See id*.

[259] *See id*. at 2. The GDPR applies not only to the EU member states but also to the EFTA States of Iceland, Lichtenstein and Norway. *See* Bernd Schmidt, *The Applicability of the GDPR within the EEA*, TECHNICALLY LEGAL (Feb. 9, 2018), https://planit.legal/blog/en/the-applicability-of-the-gdpr-within-the-eea/ [https://perma.cc/QSU4-KPYY].

[260] Jan Albrecht, *Legislative Train Schedule, General Data Protection. Practical Guidelines are Available*, EUROPEAN PARLIAMENT (July 20, 2018), http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-general-data-protection-regulation [https://perma.cc/4UWX-K6Q6].

massive record-keeping requirements).[261] As stated above, 92% of American companies considered compliance with the GDPR a top priority in 2017.[262]

A. New/Expanded Concepts

[54] The GDPR corrects four problems immediately. First, it harmonizes the laws across the EU. Second, it gives DPAs the tools they need to enforce privacy laws with the increase in maximum fines that can be assessed. Third, it expands the definition of personal data to cover advances in what machines may be able to collect in the future. Fourth, it will allow DPAs to go after companies located outside of the EU. Much of the GDPR is based on the 95 Directive. While this will make the transition easier for companies located in the EU, it will require a significant change in understanding regarding data usage for U.S. companies.

1. Regulation vs. Directive

[55] While the 95 Directive was a directive, the GDPR is a regulation.[263] Regulations have binding legal force throughout every EU member state and are directly applicable in every member state.[264] Directives describe a result that every member state must achieve, but they are free to decide how to incorporate the goal of the directive into national laws.[265]

[56] The 95 Directive had a number of weaknesses which were addressed in the GDPR. A 2009 report by the RAND corporation and sponsored by the UK's Information Commissioner's Office indicated that the 95

[261] *See id.*

[262] *See GDPR Compliance Top Priority*, *supra* note 26.

[263] *See Proposal for a Regulation*, *supra* note 257.

[264] *See Regulations, Directives, and Other Acts*, EUROPEAN UNION, https://europa.eu/european-union/eu-law/legal-acts_en [https://perma.cc/MN33-ZQPL].

[265] *See id.*

Directive led to inconsistencies between the member states' laws as each could determine on its own how the goals of the Directive were to be implemented.[266] In addition, enforcement actions were inconsistent and could result in multiple jurisdictions bringing actions for the same or similar violation.[267] The rules on cross-border transfers were outdated because of advances in technology, such as cloud storage.[268] The definitions of controllers and processors were incomplete.[269] Because the Regulation must be implemented into each member states' laws, it addresses the inconsistency problem of the 95 Directive as well as provides the likelihood that a company will only have to deal with one DPA.[270]

2. Increased Penalties

[57] One of the weaknesses of the 95 Directive was the low maximum fines permitted by member states' laws. The GDPR corrects this by substantially increasing penalties for violations of the regulation up to 4% of annual global revenue or €20 million (whichever is greater).[271]

[266] *See* NEIL ROBINSON ET AL., REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE 24 (2009), https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf [https://perma.cc/488R-WXLS].

[267] *See id.* at 35–36.

[268] *See id.* at 33–34.

[269] *See id*. at 36.

[270] *See id.* at 44. The concept of a "One-Stop-Shop" is to provide a single, uniform decision-making process in circumstances in which multiple regulators have responsibility for regulating the same activity performed by the same organization in different Member States. The WP29 has issued Guidelines on Lead DPAs (WP 244) which provide further clarity on how to determine which DPA is the lead DPA for a given controller. *See* Article 29 Data Protection Working Party, Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority EN/16 WP 244, 7–8 (Dec. 13, 2016), http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf [https://perma.cc/4XWC-3HBW].

[271] *See* GDPR, *supra* note 14, at art. 83(5).

According to its Form 10-K filed with the U.S. Securities and Exchange Commission, Facebook earned $27.638 billion in 2016,[272] which could conceivably bring sanctions of more than $1.105 billion. Google's 2017 earnings were $109.65 billion,[273] which could potentially result in a fine of $4.386 billion. The examples of potential violations given on an education portal set up by one data protection service provider include "not having sufficient customer consent to process data or violating the core of Privacy by Design concepts."[274] Failure to keep adequate records, failure to notify the supervising authority of a data breach, or failure to conduct a privacy impact assessment are also subject to a substantial penalty of up 2% of annual global turnover or €10 Million (whichever is greater).[275] This would significantly increase the motivation of tech companies to comply with the new law.

3. Expanded Definition of Personal Data

[58] Another issue addressed in the GDPR is the definition of personal data to include advances in technology. The GDPR expands the definition of "personal data" by adding genetic identity and GPS data, although for the most part reiterates the 95 Directive definition:

> 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

[272] *Annual Report (Form 10-K)*, FACEBOOK (Dec. 31, 2016), https://www.sec.gov/Archives/edgar/data/1326801/000132680117000007/fb-12312016x10k.htm [https://perma.cc/QLZ7-N6GW].

[273] *Google's Revenue Worldwide from 2002 to 2017 (in Billion U.S. Dollars)*, STATISTA, https://www.statista.com/statistics/266206/googles-annual-global-revenue/ [https://perma.cc/4JLN-XL9Y].

[274] *GDPR Key Changes: An Overview of the Main Changes under GDPR and How They Differ from the Previous Directive*, EU GDPR, https://eugdpr.org/the-regulation/ [https://perma.cc/NSA5-JFRE].

[275] GPDR, *supra* note 14, at art. 83(4)–(5).

> 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;[276]

[59] Recital (26) to the GDPR also clarifies that personal data that has been pseudonymized remains personal data subject to the requirements of the GDPR.[277] Article 4(5) of the GDPR defines pseudonymization as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information."[278] It remains subject to the GDPR because it can be re-

[276] *Id.* at art. 4(1); *see also* 95 Directive, *supra* note 13, at art. 2(a).

[277] *See* GDPR, *supra* note 14, at recital 26; *see also* Matt Wes, *Looking to Comply with GDPR? Here's a Primer on Anonymization and Pseudonymization*, IAPP: THE PRIVACY ADVISOR (Apr. 25, 2017), https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/tps://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/ [https://perma.cc/5WSZ-LFJH] ("Although similar, anonymization and pseudonymization are two distinct techniques that permit data controllers and processors to use de-identified data. The difference between the two techniques rests on whether the data can be re-identified. Recital 26 of the GDPR defines anonymized data as 'data rendered anonymous in such a way that the data subject is not or no longer identifiable.' Although circular, this definition emphasizes that anonymized data must be stripped of any identifiable information, making it impossible to derive insights on a discreet individual, even by the party that is responsible for the anonymization. When done properly, anonymization places the processing and storage of personal data outside the scope of the GDPR. The Article 29 Working Party has made it clear, though, that true data anonymization is an extremely high bar, and data controllers often fall short of actually anonymizing data.").

[278] GDPR, *supra* note 14, at art. 4(5); *see also*, Wes, *supra* note 277 ("By rendering data pseudonymous, controllers can benefit from new, relaxed standards under the GDPR. For instance, Article 6(4)(e) permits the processing of pseudonymized data for uses beyond the purpose for which the data was originally collected. Additionally, the GDPR envisions the possibility that pseudonymization will take on an important role in demonstrating compliance under the GDPR. Both Recital 78 and Article 25 list pseudonymization as a method to show GDPR compliance with requirements such as Privacy by Design.").

identified with additional information, whereas, anonymized data is not subject to the GDPR.[279] Pseudonymization has the advantage of permitting data processors to use personal data with less risk to the rights of the users because the data cannot be tied to an identifiable person without additional information. For this reason, the GDPR provides that pseudonymization may be considered as one of the possible factors by controllers to "ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected."[280]

4. Extraterritoriality

[60] In general, the GDPR is intended to apply to organizations outside of the EU when its territorial and material scope conditions are met, explicitly covers a wider range of data, and includes requirements for processors in addition to controllers.[281] It sets out these specific requirements in 99 articles.[282] The following will discuss the GDPR's expanded extraterritorial scope, placing it in the context of extraterritoriality of legislation, generally.

[61] One of the main concerns, or rather points of contention, that U.S. companies have with the GDPR is its extraterritorial scope. While initially companies understood that they would be subject to European law if they

[279] There are a number of scholars in the U.S. who have argued that re-identification of anonymized information is possible. *See, e.g.*, Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 GEO. L. TECH. REV. 202, 212 (2017).

[280] *See* GDPR, *supra* note 14, at art. 6(4); *see also id.* at recital 78, art. 25 (identifying pseudonymization as a possible way to show GDPR compliance with requirements such as Privacy by Design).

[281] *See id.* at recitals 22–25, arts. 24–29*; see also* DLA Piper Global Law Firm, *EU General Data Protection Regulation—Key Changes*, [hereinafter DLA Piper, *Key Changes*] https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/1/ [https://perma.cc/N9YP-RGBU].

[282] *See* GDPR, *supra* note 14, at art. 99.

had a *data controller* in the EU,[283] they are not wholly on board with the idea that the GDPR applies to them if they do not. From a practical perspective, the focus of the new regulation's territorial scope is mainly related to where the user is located, not the processor, although either may lead to application of the EU law.[284]

[62] Previous law was ambiguous in its description of who outside of the EU was subject to the provisions of the 95 Directive and the member states' laws. [285] The GDPR makes clear that anyone processing the data of residents of the EU, regardless of whether or not they have an office in the EU, is subject to the regulation.[286] The 95 Directive had a form of extraterritorial effect through the limiting of cross-border personal data transfers from the European Union to countries found to have adequate level of data protection.[287] In addition, the 95 Directive applied to non-EU data controllers if the controller either had an establishment in the territory of an EU member state where the data processing was carried out, or where

[283] *See id.* at art. 4(7) (defining a "controller" as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; …."); *see also id.* at art. 4(8) (stating that a "processor" may process personal data "on behalf of the controller").

[284] The part of the GDPR relevant to the user's location follows:

> 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.

Id. at art. 3(2).

[285] *See, e.g.*, Dan Jerker B. Svantesson, *The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and Its Practical Effect on U.S. Businesses*, 50 STAN. J. INT'L L. 53, 62 (2014) (proposing the definition of extraterritorial jurisdiction as one which seeks to control or directly affect an object's activities outside such state's territory).

[286] GDPR, *supra* note 14, at art. 3(2).

[287] 95 Directive, *supra* note 13, at art. 25(1).

equipment in the territory of a member state was used for the processing.[288] With respect to personal data, Article 4 of the 95 Directive provided that the applicable law is the law of the member state in which the data processor has an establishment and where the processing takes place.[289] If the non-EU data controller did not have such an establishment, it could still be subject to EU law if it made use of equipment on the territory of a member state for its data processing (other than for mere "transit" of the data).[290] In this case, it was required to designate a representative established in the territory of such member state.[291] As an illustration, the Court of Justice of the European Union found that it had jurisdiction under the 95 Directive in the now-famous *Google Spain* "right to be forgotten" case,[292] with respect to the California-headquartered (and Delaware-incorporated) corporation Google Inc. and its search engine. Google Inc. had Google Spain SL as an establishment in the European Union, the latter of which raised funds through advertising used to finance the search engine.[293]

[63] The GDPR, does in fact, go much further. Not only does it apply to processing in the context of activities of a data controller or a processor in the European Union,[294] but it also applies to processing by controllers or

[288] *Id.* at art. 4(1)(a). Svantesson comments that this provision provides "considerable scope for extraterritoriality," especially given the possibility for EU member states to adopt broad ranges of views as to what constitutes being "established." *See* Svantesson, *supra* note 285, at 66.

[289] *Id.* at art. 4(1).

[290] *See id.* at art. 4(1)(c); *see also* CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW, 124–125 (2013) (stating that this provision, which bases jurisdiction on the use of "equipment" and not on nationality or residency "can lead to conflicts of law").

[291] *Id.* at art. 4(2).

[292] *See generally* Case C-131/12Google Spain SL v. Agencia Española de Proteccíon de Datos (2014).

[293] *See* Voss, *The Right to Be Forgotten*, *supra* note 142, at 3, 4.

processors not established in the European Union, if such processing relates to the offering of goods or services (whether free or for-payment) to EU data subjects, or involves the monitoring of their behavior, insofar as such behavior takes place in the European Union.[295] However, one commentator claims that the requirement of appointing a representative, pursuant to GDPR Article 27, might lead to stable arrangements, in which case the establishment clause of Article 3(1) may be triggered so as to be "likely to even absorb the remaining field of application of the two alternatives posed under Article 3(2)."[296] The extraterritorial effect may also be extended by practice through what has been called the "Brussels effect": "the GDPR is likely to *de facto* influence the setting of global standards for online data protection significantly by virtue of its territorial scope, as data controllers can be expect to adjust their compliance according to the highest level of data protection required from them."[297]

[64] It bears repeating that many legal systems, including the U.S., extend the reach of their laws outside of the territorial boundaries through long arm statutes and the concept of minimum contacts.[298] In fact, many U.S. states enforce their breach notification laws on companies headquartered in other states (or outside of the United States, for that matter), if the entity "conducts business" in the state.[299]

---

[294] GDPR, *supra* note 14, at art. 3(1).

[295] *Id.* at art. 3(2).

[296] Merlin Gömann, *The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement*, 54 COMMON MKT. L. REV. 567, 575 (2017).

[297] *Id*., at 568 (citing Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012)).

[298] *See* Timothy M. Banks, *The Long-Arm of Data Protection and Data Production Laws*, IAPP.ORG (May 20, 2014), https://iapp.org/news/a/the-long-arm-of-data-protection-and-data-production-laws/ [https://perma.cc/CR5K-4RQR].

[299] *Id.*

[65] Extraterritorial application of U.S. antitrust law is well established.[300] With respect to the Sherman Act, the court in *U.S. v. Aluminum Company of America* found jurisdiction over acts that occurred outside of the U.S. but had consequences within U.S. borders.[301] In January 2017, the FTC and DOJ updated the 1995 Antitrust Guidelines for International Enforcement and Cooperation to clarify and broaden the scope of enforcement of U.S. antitrust laws against foreign entities.[302] In addition, a number of decisions in recent years have interpreted the Foreign Trade Antitrust Improvements Act as applying U.S. antitrust law to anticompetitive conduct occurring outside of the U.S.[303] The update makes clear the expanded scope of the extraterritorial application of U.S. antitrust law. Thus, it would be difficult to argue that the EU cannot enforce laws for conduct occurring outside of its territorial boundaries.[304]

---

[300] *See generally* Richard W. Beckler & Matthew H. Kirtland, *Extraterritorial Application of U.S. Antitrust Law: What Is a "Direct, Substantial, and Reasonably Foreseeable Effect" Under the Foreign Trade Antitrust Improvements Act?*, 38 TEX. INTL. L. J. 11 (2003).

[301] United States v. Aluminum Co. of Am., 148 F.2d 416, 443 (2d Cir. 1945).

[302] *See generally* ANTITRUST GUIDELINES FOR INTERNATIONAL ENFORCEMENT & COOPERATION, § 1 (U.S. Dep't Just. & Fed. Trade Comm'n 2017).

[303] Jennifer B. Patterson & Terri A. Mazur, *Recent Developments in the Extraterritorial Reach of the US Antitrust Laws*, ARNOLDPORTER.COM (Aug. 13, 2014), https://www.arnoldporter.com/-/media/files/ks-imported/20140813_r_pattersonmazurinsidecounselarticleaugust132014pdf.pdf? [https://perma.cc/3VNR-MYYB].

[304] This extraterritorial effect might be criticized as "regulatory overreach" or as an "intrusion into State sovereignty," which are not new concerns, even in the data protection context. *See* Gömann, *supra* note 296, at 568. Yet, not only do various grounds for jurisdiction exist under international custom, but extraterritoriality effects are allowed in other areas such as international economic law. *See, e.g.*, Svantesson, *supra* note 285, at 79–82. One scholar states that, "Whereas the enactment of extraterritorial legislation was once viewed as the preserve of the United States and as provoking the wrath of the EU; today—so the argument goes—extraterritoriality is a phenomenon that is both tolerated by the EU and that is increasingly practiced in its name." Joanne Scott, *Extraterritoriality and Territorial Extension in EU Law?*, 62 AM. J. COMP. L. 87, 88

[66] Despite this, it is likely that U.S. tech companies will seek to avoid the extraterritorial jurisdiction of the GDPR. In *Facebook Belgium v. Belgian Privacy Commission*,[305] Facebook argued that Facebook Ireland was the sole data controller with respect to Belgian data subjects, and that only the Irish Privacy Commission, to the exclusion of the Belgian Privacy Commission, had jurisdiction.[306] The initial suit against Facebook argued that its non-user tracking mechanisms violated EU and Belgian privacy laws.[307] The Belgian Privacy Commission asked the Court to stop Facebook from placing cookies on non-users' browsers without "sufficient and adequate information" about Facebook's practice and how they use the data,

(2014). Examples of these include Anti-trust or competition law (such as regulations of the United States and the European Union), securities laws (including the Sarbanes-Oxley Act), and taxes, among others. *See* JOHN H. JACKSON, SOVEREIGNTY, THE WTO, AND CHANGING FUNDAMENTALS OF INTERNATIONAL LAW 22 (2006). Nonetheless, Scott argues that "while the EU only very rarely enacts extraterritorial legislation, it makes frequent recourse to a mechanism that may be labeled "territorial extension," allowing it to govern activities not on its territory. Scott, *supra* at 89. Furthermore, she indicates that there "are countless U.S. measures that give rise to territorial extension." *Id.* at 120. Scott defines "territorial extension" as "[t]he application of a measure is triggered by a territorial connection but in applying the measure that regulator is required, as a matter of law, to take into account conduct or circumstances abroad." *Id*. at 90. Moreover, according to the U.S. Department of Commerce's Bureau of Economic Analysis, the fines and penalties resulting from application of domestic law to foreign corporations in the areas of antitrust (and EU competition law), anti-bribery legislation and other (primarily financial) legislation have resulted in positive net U.S. unilateral transfers (after deduction for amounts paid, mainly to the European Commission and member state competition authorities in competition law cases) of $ 25.635 billion from 1999-2013. *See* Christopher L. Bach, *Fines and Penalties in the U.S. International Transactions Accounts*, BEA 57 (July 2013), https://apps.bea.gov/scb/pdf/2013/07%20July/0713_fines_penalties_international_accounts.pdf [https://perma.cc/7MCQ-H2V4]. Seemingly, this leaves the United States with little about which to grumble in the context of GDPR extraterritoriality.

[305] Tribunal de Première Instance [Dutch-Speaking Ct. of First Instance Brussels], Nov. 9, 2015, 15/57/C (Belg).

[306] *Id*. at 3–4, 9.

[307] *Id.* at 10.

and to cease collecting the data cookies through their social plug-ins.[308] Facebook argued that neither Belgian nor EU law applied in this situation because it had met the establishment test allowing Ireland to have jurisdiction over data processing issues.[309] Although Facebook lost this argument in the lower court,[310] the Court of Appeal of Brussels overruled the lower court's decision, and held that the Belgian courts lacked jurisdiction over Facebook because its European headquarters were located in Ireland.[311]

[67] Following an interlocutory procedure at the end of 2017, the case was then sent back to the lower court where it found that the party having the financial decision-making capacity for the processing of personal data of data subjects in Belgium was the Chief Operating Decision Maker of Facebook Inc., and thus Facebook Inc. was a co-controller, and that the Belgian lower court had jurisdiction for the three Facebook entities with respect to Belgian data subjects, and ruled in favor of the Belgian Privacy Commission and against Facebook.[312]

[68] As seen in the Belgian case, the determination of who is or is not a data controller is an arduous one.[313] Under the GDPR, however, Articles

[308] *Id.* at 11.

[309] *Id.* at 9.

[310] Tribunal de Première Instance [Dutch-Speaking Ct. of First Instance Brussels], Nov. 9, 2015, 15/57/C (Belg.), at 32–33. For a short discussion of the lower court decision, *see* Mila Owen, *Belgian Court Demands that Facebook Stop Tracking Non-Members*, JOLT DIGEST (Dec. 10, 2015), http://jolt.law.harvard.edu/digest/belgian-court-demands-that-facebook-stop-tracking-non-members [https://perma.cc/6YCE-V6QA].

[311] Hof van beroep [HvB] [Court of Appeal] Brussels, 18th ch. June 29, 2016, 2016/KR/2 (Belg.), https://www.navigator.nl/document/id4cb1ef4fdda64bbc8727c16f4eb7d2f8/ecli-nl-xx-2016-128-hof-van-beroep-brussel-29-06-2016-nr-2016kr2 [https://perma.cc/N3SP-F3ZK].

[312] Tribunal de Première Instance [Dutch-speaking Court of First Instance], Brussels, Feb. 16, 2018, 2016/153/A (Belg.).

4(7) and 4(8) would clearly define Facebook as a data controller because the "purpose and means" of the data processing are determined in the U.S., not Ireland.[314] However, the subsequent *Wirtschaftsakademie Schleswig-Holstein GmbH* ruling, issued on June 5, 2018, has simplified matters, allowing for the law of the relevant establishment of the parent company to apply.[315]

[69] Companies might also be tempted to place a choice of law provision in their terms of use making U.S. law applicable to any dealings with a U.S. company's website, hoping to avoid the requirements of the GDPR. However, this was anticipated by the GDPR. Even if a company is not established in the EU, it is expressly subject to the GDPR if it processes information regarding data subjects in the EU either through the offering of goods or services to them[316] or by monitoring their behavior (e.g., targeted marketing), to the extent that such behavior occurs in the EU.[317]

5. Ongoing Requirements/Culture Change

[70] It should be noted that there is no checklist that a company can go through to certify that it has complied with the GDPR because the requirements are ongoing. Compliance with the GDPR will require a complete culture change for U.S. companies because the rights afforded data subjects in the EU are not rights that American data subjects have, nor that U.S. companies have been operating under. The shift in thinking will be from an ownership model to a leasing model. Essentially, all employees of a business will need to change their outlook from t*his is the company's data* to the idea that *this data belong to the data subject and we are just*

[313] Tribunal de Première Instance [Dutch-speaking Court of First Instance], Nov. 9, 2015 15/57/C (Belg.).

[314] GDPR, *supra* note 14, at art. 4(7)–(8).

[315] *See supra* Section III(A)(2)(b).

[316] *Id.* at art. 3(2)(a).

[317] *Id.* at art. 3(2)(b), recital 24.

leasing it. A company can only collect and process a user's data to the extent explicit consent is given for their activities and *such consent can be withdrawn at any time*.[318] An individual's rights will generally trump a company's rights to an individual's data. The following section will describe some of the more important provisions of the GDPR.

B. Important Provisions of the GDPR

1. Applicability to Controllers and Processors

[71] Only controllers had direct legal responsibility under the 95 Directive.[319] Under the GDPR, both controllers and processors are responsible for compliance. Article 4 defines data controllers and data processors as follows:

> (7) "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
> (8) "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[320]

For example, if a company A sells books to consumers and uses company B to track the orders and obtain payment information from the consumers, company A is the controller and company B is the processor.[321]

---

[318] *Id.* at art. 7(3).

[319] 95 Directive, *supra* note 13, at art. 6(2).

[320] GDPR, *supra* note 14, at art. 4(7)–(8).

[72] The GDPR treats the data controller as the principal party for responsibilities such as collecting consent, managing consent-revocation, enabling right to access, etc. A data subject who wishes to revoke consent for his or her personal data therefore will contact the data controller to initiate the request, even if such data lives on servers belonging to the data processor. The data controller, upon receiving this request, would then proceed to request that the data processor remove the revoked data from their servers.[322]

[73] Although the controller is primarily responsible for compliance, the processor can also be liable under the GDPR for noncompliance.[323] Because of the extraterritorial jurisdiction of the GDPR, this change to the law broadens which companies may be found liable for failing to honor rights given to European users.

2. The Right to be Forgotten

[74] As described in Section III(A)(1)(c) above, the right to be forgotten was established in the *Google Spain* case.[324] While this right was mentioned in the 95 Directive, the GDPR expands this right to be consistent with the ruling in *Google Spain*.[325] Article 17 reads:

> 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the

[321] *Data Controllers and Processors*, GDPR EU.ORG, https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/ [https://perma.cc/WWU2-897H].

[322] *Id*

.

[323] *See* GDPR, *supra* note 14, at art. 28(4) (providing information only for the liability of controllers).

[324] *See supra* Section III(A)(1)(c).

[325] *See* GDPR, *supra* note 14, at art. 17.

obligation to *erase personal data without undue delay* where one of the following grounds applies:

a) the personal data are *no longer necessary in relation to the purposes for which they were collected* or otherwise processed;
b) the data subject *withdraws consent* on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
c) the data subject *objects* to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
d) the personal data have been *unlawfully processed*;
e) the personal data have to be erased for compliance with a *legal obligation* in Union or Member State law to which the controller is subject;
f) the personal data have been collected in relation to the offer of *information society* services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.[326]

[326] *Id.* (emphasis added).

Although this is not a new requirement, companies will need to have better procedures in place to comply with European users' right to be forgotten.[327] Companies will now need to inform data subjects not only of their ability to correct information about themselves,[328] but also to have information deleted.[329] If a data subject withdraws their consent, and that consent has served as the legal basis for processing their data, their data must be deleted.[330]

3. Right to Data Portability

[75] The right for users to transfer their data to a new controller (e.g., one budgeting app to another) is new in the GDPR. Article 20 reads:

> 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and *machine-readable format* and have the *right to transmit those data to another controller* without hindrance from the controller to which the personal data have been provided, where:
>   a. the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
>   b. the processing is carried out by automated means.
> 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

[327] *See supra* Section III(A)(1)(c)

[328] *See* GDPR, *supra* note 14, at art. 16.

[329] *See id.* at art. 17.

[330] *Cf. id.*

> 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
> 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.[331]

[76] This requirement will permit users to transfer their data or obtain a copy of their data in machine-readable format.[332] In most cases, the controller will not be permitted to charge for this service and will need to provide the information within one month of the request.[333] There is no corresponding right in under U.S. law.[334] This new provision will actually help smaller companies take advantage of data records created by their competitors. Although banks in some member states in the EU were previously subject to this requirement,[335] users who were reluctant to switch to a new social media platform, for example, can now take their data with them.

4. Lawful Basis for Processing

[77] While the requirements for lawful basis echo those in the 95 Directive, the GDPR makes it more difficult for organizations to process

[331] *Id.* at art. 20 (emphasis added).

[332] *See Id.*

[333] *See* GDPR, *supra* note 14, at art. 12(3), (5).

[334] *See* Tim Rollins, *Could the US Have Its Own GDPR?*, EXTERRO (Mar. 23, 2018), https://www.exterro.com/blog/could-the-us-have-its-own-gdpr/ [https://perma.cc/WE4E-68PC].

[335] *See* Bruce Bennett et al., *Overlap Between the GDPR and PSD2*, INSIDE PRIVACY (Mar. 16, 2018), https://www.insideprivacy.com/financial-institutions/overlap-between-the-gdpr-and-psd2/ [https://perma.cc/CH7L-D58E].

personal data for a new purpose due to its description of *compatible* purposes.[336] Article 6(1) reads:

> Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> a. the data subject has given *consent* to the processing of his or her personal data for one or more specific purposes;
> b. processing is necessary for the performance of a *contract* to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
> c. processing is necessary for compliance with a *legal obligation* to which the controller is subject;
> d. processing is necessary in order to *protect the vital interests* of the data subject or of another natural person;
> e. processing is necessary for the performance of a *task carried out in the public interest* or in the exercise of official authority vested in the controller;
> f. processing is necessary for the purposes of the *legitimate interests* pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights

[336] *See* GDPR, *supra* note 14, at art. 6(4) (Where personal data are to be processed for a new purpose, the controller must consider whether the new purpose is "compatible" with the original purpose considering the following factors:

> a. any link between the original purpose and the new purpose;
> b. the context in which the data have been collected, including the controller's relationship with the data subjects;
> c. the nature of the personal data, in particular, whether Sensitive Personal Data are affected;
> d. the possible consequences of the new purpose of processing for data subjects; and
> e. the existence of appropriate safeguards (e.g., encryption or pseudonymisation).)

> and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[337]

[78] If specific consent is not given for the processing, the company's use of the data must fall within one of the above categories (b – f) and organizations will most likely need to explain how the individual's privacy rights are outweighed by such use. This is not a requirement under U.S. law and for that reason may present a stumbling block for U.S. corporations wishing to process EU generated information the same way they process U.S.-generated information.

5. Data Protection Officer

[79] As mentioned in Section IV(A) above, regardless of whether a data protection officer (DPO) is required for an organization, appointing one will assist the company in achieving compliance. The DPO would ensure proper consent, privacy by design, conduct privacy impact assessments, respond to user requests, and serve as the point of contact with local DPAs. Article 37 of the GDPR reads:

> 1. The controller and the processor shall designate a data protection officer in any case where:
>   a. the processing is carried out by a *public authority* or body, except for courts acting in their judicial capacity;
>   b. the core activities of the controller or the 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
>   c. the core activities of the controller or the processor consist of processing on a large scale

[337] *See* GDPR, *supra* note 14, at art. 6(1) (emphasis added).

> of *special categories of data* pursuant to Article 9 or personal data relating to *criminal convictions* and offences referred to in Article 10.
>
> 2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.
> 3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.
> 4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.
> 5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.
> 6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
> 7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.[338]

[80] In order to comply with the GDPR, best practices for companies collecting and processing data in Europe will most likely include appointing a DPO.[339] Although a DPO is only required for public bodies or when a

[338] *See* GDPR, *supra* note 14, at art. 37 (emphasis added).

[339] *See* Tim Bell, *Is Article 27 the GDPR's 'Hidden Obligation'?*, IAPP (May 3, 2018), https://iapp.org/news/a/is-article-27-the-gdprs-hidden-obligation/

company's "core [processing] activities [. . .] require regular and systematic monitoring of data subjects on a large scale; or [where its] core activities [. . .] consist of the processing of sensitive data on a large scale,"[340] most tech companies do engage in the large-scale monitoring of individuals. The DPO will need to ensure that European users' data is sufficiently protected and that the data controller complies with the GDPR.[341] The DPO will need to be an expert in data protection law,[342] thus, it is unlikely that current IT professionals will meet this definition. In addition, the DPO must be independent,[343] so an IT or marketing professional within the corporation would most likely have a conflict of interest, unless released from his or her other obligations. The DPO is responsible for reporting data breaches to EU authorities within 72 hours of detection of the breach.[344] In addition, if the company processes data from EU residents in connection with the offer of products or services to them or monitors their behavior in the EU, and it is not established in the EU, it will also be required to have a representative located in the EU.[345] This requirement was previously optional in the EU

[https://perma.cc/BTS2-X6JQ] ("The purpose of this is simple: It ensures that EU citizens will be able to contact the controllers and processors outside of Europe that hold their personal data, without having the potentially confusing, difficult and costly efforts required to contact them at their base."). *See generally* GDPR, *supra* note 14, at art. 27 (requiring companies without offices in the EU that monitor or process the personal data of users within the EU to appoint an EU-based representative to be the contact person for the local DPA).

[340] *See* GDPR, *supra* note 14, at art. 37.

[341] *See id.* at art. 39

[342] *See id.* at art. 37(5).

[343] *See Data Protection Officer (DPO)*, EUR. DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en [https://perma.cc/96CL-7J9F].

[344] *See* GDPR, *supra* note 14, at art. 33 (explaining this requirement applies "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.").

[345] *See id.* at arts. 3, 27.

under most member states' laws, except where it was required of processers in Germany.[346] In addition to advising the company on all things GDPR, DPOs will be responsible for the massive record-keeping requirements.[347]

6. Affirmative Consent

[81] One of the bases for lawful processing is consent. Article 7 reads:

> 1. Where processing is based on consent, the controller shall be able to *demonstrate* that the data subject has consented to processing of his or her personal data.
> 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using *clear and plain language*. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
> 3. The data subject shall have the *right to withdraw* his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. *It shall be as easy to withdraw as to give consent*.
> 4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[348]

[346] *See* DLA Piper, *Key Changes*, *supra* note 281.

[347] *See id.*

[348] GDPR, *supra* note 14, at art 7 (emphasis added).

The GDPR expands the consent requirements by requiring proof of such consent.[349] The 95 Directive merely required the user to signify agreement.[350] Consent is defined in the GDPR as: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data."[351] The GDPR use the initial language from the 95 Directive, but added "unambiguous."[352] As mentioned above, one *lawful basis* for the processing of data is consent.[353] In the event a U.S. company cannot provide a contractual basis[354] or legitimate interest[355] for the processing of personal data, they will need to provide proof of consent. The GDPR sets the age of consent at 16.[356] Companies will need to obtain and document[357] the affirmative consent in plain language[358] of its users to the collection, processing, and storing of their

[349] *See* Gabe Maldoff, *Top 10 Operational Impacts of the GDPR: Part 3—Consent*, IAPP: THE PRIVACY ADVISOR (Jan. 12, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/ [https://perma.cc/EM3X-PQBL].

[350] *See* 95 Directive, *supra* note 13, at art. 2(h), art. 7.

[351] *See* GDPR, *supra* note 14, at art. 4(11).

[352] *Compare* 95 Directive, *supra* note 13 (stating the proposition in two separate sections), *with* GDPR, *supra* note 14, at art. 4(h) (stating the proposition in one clear and concise definition).

[353] *See* discussion *supra* Section IV(B)(6).

[354] *See* GDPR, *supra* note 14, at art. 6(1)(b).

[355] *See id.* at art. 6(1)(f).

[356] *See id.* at art. 8 (stating that member states are able to set a lower age–not lower than 13 years—but those under the set age will need to comply with additional requirements similar to COPPA, such as parental consent).

[357] *See id.* at art. 7.

[358] *See id.*

personal data, and provide an easy mechanism for the users to withdraw their consent.[359]

[82] The GDPR expressly provides that silence, inactivity, and pre-checked boxes will not meet this requirement of affirmative consent.[360] Also, unlike U.S. law, the individual retains the right to revoke the consent at any time.[361] An important issue that this raises is what is required of U.S. companies that have already collected and processed information of EU data subjects.[362] Will verifiable consent need to be obtained for data maintained after May 25, 2018? It seems unlikely that U.S. companies will have adequate records to obtain this consent given that they previously relied on individual's opting out of the collection of their information, but it is also just as likely that DPAs will require this. In essence, if the consent obtained prior to the GDPR's application was *GDPR-compliant* then new consent would not be necessary. However, if the previous consent was not GDPR-compliant, then new consent that complies with the GDPR would need to be obtained.

[83] Another significant aspect of the consent requirements is that the data subjects must be informed about how the data will be used at the time of collection.[363] This raises issues regarding the ability to share and sell the information, as secondary uses may not be known at the time of collection.

---

[359] *See* GDPR, *supra* note 14, at art. 7(3).

[360] *See id.* at recital 32.

[361] *See id.* at art. 7(3).

[362] *See* Todd Ehret, *U.S. Firms are Still Uunprepared for Looming EU Data Privacy Rules*, REUTERS (Feb. 13, 2018, 12:30 PM), https://www.reuters.com/article/bc-finreg-data-privacy-rules/u-s-firms-are-still-unprepared-for-looming-eu-data-privacy-rules-idUSKCN1FX2D2 [https://perma.cc/U7E3-2PHL] ; *see, also Eye on Discovery—Five Steps to Take Now to Prepare for the General Data Protection Regulation*, CONSILIO, http://www.consilio.com/resource/eye-discovery-five-steps-take-now-prepare-general-data-protection-regulation/ [https://perma.cc/M6AG-BSK8] .

[363] *See* GDPR, *supra* note 14, at recital 32.

It seems that the drafters of the GDPR were aware of this practice and sought to stop it. The notice asking for consent will need to be very detailed in its disclosures. Additionally, data subjects must also be informed that they have the right to file a complaint with the company's DPO.[364]

7. Data Protection by Design

[84] The idea of data protection by design and default is that privacy needs to be considered prior to the time the data is collected and processed in the first place.[365] This is a completely new requirement under the GDPR. Article 25 reads:

> 1. *Taking into account* the state of the art, the *cost* of implementation and the nature, scope, context and *purposes of processing* as well as the *risks of varying likelihood and severity for rights and freedoms of natural persons* posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, *implement appropriate technical and organisational measures*, such as *pseudonymisation*, which are designed to implement data-protection principles, such as *data minimisation*, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and *protect the rights of data subjects*.[366]

[364] *See* Miriam C. Beezy & Stephanie A. Lucas, *Compliance with the EU's General Data Protection Regulation and U.S. Discovery Law*, 72 INTA BULLETIN 1, 6 (2017), https://www.inta.org/Advocacy/Documents/2017/Article%20-%20Compliance%20with%20the%20EU_S%20General%20Data%20Protection%20Regulation%20and%20US%20Discovery%20Law.pdf [https://perma.cc/XE2Z-GCKZ].

[365] *See, e.g.*, GDPR, *supra* note 14, at art. 25.

[366] *See id.* (emphasis added).

[85] An example of designing your processing with data protection in mind would be pseudonymisation.[367] This will present significant challenges for those using machine learning algorithms that infer details based on patterns discovered in massive amounts of data. As it is not always possible to know the criteria that the machine has "learned" and is now incorporating, it is difficult to see how it can be disclosed.[368] Although the idea behind privacy by design is to incorporate privacy in the developmental stages of data processing, Privacy Impact Assessments (PIA) can further guide companies in making changes when reviewing current systems. It will also be likely that reports will be maintained on how privacy by design was implemented by the company to demonstrate compliance with the GDPR.[369]

8. Impact Assessments

[86] The 95 Directive did not require privacy or data protection assessments prior to processing, nor is there any similar requirement under U.S. law.[370] However, this new requirement in the GDPR is intended to help organizations identify potential issues with their processing of user data.[371] Article 35(1-3) reads:

> 1. Where a type of processing in particular *using new technologies*, and taking into account the nature, scope, context and purposes of the processing, is *likely to result*

[367] *See id.*

[368] *See, e.g.*, MAYER-SCHÖNBERGER & CUKIER, *supra* note 104, at 109 (giving an example of how Google's Street View cars gathered a variety of information besides that which was within its original purpose).

[369] *See generally* Ira Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409 (2011) (discussing the ability to regulate privacy by design).

[370] *See* 95 Directive, *supra* note 13; *see* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE iii–v (2012) (recommending, but not requiring, privacy and data protections for the United States).

[371] *See* GDPR, *supra* note 14, at art. 35.

> *in a high risk to the rights and freedoms of natural persons*, the controller shall, *prior to the processing*, carry out an *assessment of the impact* of the envisaged processing operations on the *protection of personal data*. A single assessment may address a set of similar processing operations that present similar high risks.
> 2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
> 3. A data protection impact assessment referred to in paragraph 1 shall in particular *be required* in the case of:
> a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on *automated processing*, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
> b. processing on a *large scale of special categories* of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
> c. a *systematic monitoring of a publicly accessible area on a large scale*.[372]

[87] The idea is that appropriate safeguards can be instituted when deficiencies are discovered. Rather than relying on individuals to evaluate the risks in sharing their data, some of the burden is placed on the controller.[373] Specifically, Article 35(7) requires that the PIA

[372] *Id.* (emphasis added)

[373] *See* Claudia Quelle, *The Data Protection Impact Assessment, or: How the General Data Protection May Still Come to Foster Ethically Responsible Data Processing* (Nov. 25, 2015), https://ssrn.com/abstract=2695398 [https://perma.cc/KVB6-ECRX] (making the case that the data protection impact assessment bakes in a privacy analysis by requiring the review to include risks to the rights and freedoms of individuals as opposed to just the).

> shall contain at least:
>
> 1. a systematic *description of the envisaged processing* operations and the *purposes of the processing*, including, where applicable, the legitimate interest pursued by the controller;
> 2. an *assessment of the necessity and proportionality* of the processing operations in relation to the purposes;
> 3. an *assessment of the risks to the rights and freedoms of data subjects* referred to in paragraph 1; and
> 4. the *measures envisaged to address the risks*, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.[374]

[88] PIAs must be documented and in accordance with any additional requirements established by the DPA.[375] One of the issues with respect to this requirement is the inherent inability to identify specific risks when machine learning is involved as mentioned above. Because machines may be making decisions based on factors which are not revealed outside of the *black box*, it is not possible to anticipate an exact risk (although certainly the potential for discrimination in general should be anticipated when engaged in any type of profiling).[376]

---

[374] GDPR, *supra* note 14, at art. 35(7) (emphasis added).

[375] *See id.* at art. 35(7), (11).

[376] One of the reasons the GDPR may be requiring explanations is because of the potential for discrimination.

For a discussion on how machine learning that results in discriminatory decision, *see, e.g*, MAYER- SCHÖNBERGER & CUKIER, *supra* note 104 at 153–54 (stating that many secondary uses of data are not considered when it is first collected because it is not

9. Profiling

[89] One provision of the GDPR that is very different from U.S. law, is the requirement under Article 22 that European users have the right to know how their personal information is being processed when an automated decision is made about them.[377] These automated decisions are known as

known to exist yet); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 5, 14–15 (2014) (discussing how machine learning can result in discriminatory decisions generally); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 101, 136–39 (2004); Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. ONLINE 41, 42–44 (2013) (describing the transparency paradox, identity paradox, and the power paradox); Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2021–22, 2027–28 (2013) (focusing on the nuance of privacy regulation and some of the consequences of that nuance); EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, at 1–2, 7, 45–47, 51–53, 59–60, 64–65 (May 1, 2014) (offering a summary of what big data is and conclusions moving forward); FED. TRADE COMMISSION, DATA BROKERS: A CALL FOR TRANSPARENCY 1, 55–56 (2014). For a discussion on how machine learning used by public bodies can result in discrimination, *see* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact,* 104 CALIF. L. REV. 671, 688, 720, 726 (2016); Fred H. Cate & Viktor Mayer-Schönberger, *Notice and Consent in a World of Big Data*, 3 INT'L DATA PRIVACY L. 67, 67–73 (2013); Christopher W. Clifton et al., *Data Mining and Privacy: An Overview*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS DISCIPLINARY CONVERSATION 191, 203 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006) (explaining that, without access to the underlying data and logic of the "No Fly" program, individual's ability to challenge inclusion on list is impaired); Melissa de Zwart et al., *Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK*, 37 U. NEW S. WALES L. J. 713, 718 (2014); Kimberly A. Houser & Debra Sanders, *The Use of Big Data Analytics by the IRS: Efficient Solution or the End of Privacy as We Know It?*, 19 VAND. J. ENT. & TECH. L. (2017); FED. TRADE COMMISSION, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION?: UNDERSTANDING THE ISSUES 1, 28 (2016) [hereinafter FTC Big Data]; *cf.* I. Bennett Capers, *Rethinking the Fourth Amendment: Race, Citizenship, and the Equality Principle*, 46 HARV. C.R-C.L. L. REV. 1, 17 (2011) (discussing racial profiling generally); MAYER-SCHÖNBERGER & CUKIER, *supra* 104, at 154 (Google Street View opt-out);.

[377] *See* GDPR, *supra* note 14, at art. 22.

profiling.[378] Companies must not only be able to explain how the decisions are being made, but also must provide a mechanism to have such activities stopped.[379] Article 22 reads:

1. The data subject shall have the *right not to be subject to a decision based solely on automated processing*, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
    a. is necessary for entering into, or performance of, a contract between the data subject and a data controller;
    b. is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
    c. is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the *data controller shall implement suitable measures to safeguard the data subject's rights and freedoms* and legitimate interests, *at least the right to obtain human intervention* on the part of the controller, to express his or her point of view and to contest the decision.
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(2)(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.[380]

[378] *See id.* at art. 4(4).

[379] *See id.* at art. 22.

[380] *Id.* (emphasis added).

[90] This provision expands upon what was in the 95 Directive.[381] According to Article 4(4) of the GDPR, profiling:

> consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.[382]

According to Veale and Edwards, the right to not be subject to an automated decision was rarely invoked under the 95 Directive.[383] However, they point out how the *right to an explanation* may be problematic in terms of compliance.[384] This is especially difficult as scholars have noted that many times algorithms are programmed to learn over time.[385] What this means is that the purpose for which the pattern recognition algorithm is set up changes as the algorithm incorporates massive amounts of data.[386] If the company is unable to see *inside the black box*, it will not be able to explain exactly on what criteria a decision was made.[387] As Article 22(4) limits

[381] *See* 95 Directive, *supra* note 13, at. recital 41.

[382] GDPR, *supra* note 14, at art. 4(4).

[383] *Cf.* Michael Veale & Lilian Edwards, *Clarity Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision Making and Profiling*, 34 COMPUTER L. & SECURITY REV. 398, 398–99 (2018) (describing that the intent of the 95 Directive was to "respond to fears in the early days of digitization that automated […] decisions might prejudice access to important facilities").

[384] *See id.* at 399.

[385] *See id.*

[386] *See* de Zwart et al., *supra* note 376, at 718.

automated decision-making and profiling based on special categories (such as race and religion), this may severely restrict the use of machine learning algorithms.[388]

10. Security Requirements

[91] Because of the recent clarification of the definition of personal data, both by the ECJ and the GDPR,[389] companies will now need to provide the same level of protection for IP addresses and GPS information as they do for names and social security numbers. The GDPR expanded the security requirements in that both the processor and controller must assure the security of the data.[390] While the 95 Directive left it to the controller to determine appropriate security measure,[391] the GDPR is more prescriptive in its approach. Unlike U.S. law, which defines required security as *reasonable measures*,[392] the GDPR provides a description of potential measures that can be taken to protect data. Article 32 reads:

> 1. *Taking into account* the state of the art, the *costs* of implementation and the nature, scope, context and *purposes of processing* as well as the *risk of varying likelihood and severity for the rights and freedoms of*

[387] *See* FTC Big Data, *supra* note 376, at 28. There is always a concern that an algorithm, while not initially set up to use factors such as race or religion, may result in targeting certain groups based on associations created as the algorithm learns.

[388] *See* GDPR, *supra* note 14, at arts. 9, 22; *see* James C. Cooper, *Separation Anxiety*, 21 VA. J. L. & TECH. 1, 1 (2017).

[389] *See* GDPR, *supra* note 14, at art. 4(1).

[390] *See* P.T.J. Wolters, *The Security of Personal Data Under the GDPR: A Harmonized Duty or a Shared Responsibility?*, 7 INT'L DATA PRIVACY L. 165, 165 (2017).

[391] *See id.* at 165, 168.

[392] *See* Elizabeth A. Brasher, Note, *Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation*, 18 COLUM. BUS. L. REV. 209, 225 (2018).

natural persons, the controller and the processor shall implement appropriate technical and organisational measures *to ensure a level of security appropriate to the risk*, including inter alia as appropriate:

a. the *pseudonymisation and encryption* of personal data;
b. the ability to *ensure the ongoing confidentiality*, integrity, availability and resilience of processing systems and services;
c. the *ability to restore* the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d. a *process for regularly testing*, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.[393]

[393] GDPR, *supra* note 14, at art. 32 (emphasis added).

[92] In addition to calling out the possibility of encryption and/or pseudonymisation of personal data, it seems likely that such security measures will also include "a combination of firewalls, log recording, data loss prevention, malware detection and similar applications."[394] Article 25 of the GDPR requires companies to implement data protection principles such as data minimization and ensure that only personal data that is necessary for each specific purpose is processed.[395] Article 25 permits certification as evidence of compliance with Article 25.[396] The European Data Protection Board has issued guidelines for certification,[397] but has not yet listed any approved certification mechanisms on their website.[398] Furthermore, security standards set forth by relevant EU member states' agencies and by the European Union Agency for Network and Information Security (ENISA) should be met.[399]

[394] *See* DLA Piper, *Key Changes* , *supra* note 281.

[395] *See* GDPR, *supra* note 14, at art. 25.

[396] *See id.* at art 25(3) ("An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article").

[397] European Data Protection Board, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, May 25, 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_1_2018_certification_en.pdf [https://perma.cc/HJ49-UT6W].

[398] European Data Protection Board, *Certification mechanisms, seals and marks*, EUROPEAN DATA PROTECTION BOARD, https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en [https://perma.cc/9CWH-J48F].

[399] *See generally* EUROPEAN UNION AGENCY NETWORK & INFORMATION SEC., PRINCIPLES AND OPPORTUNITIES FOR A RENEWED EU CYBERSECURITY STRATEGY (2017), https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-input-to-the-css-review-b/view [https:/./perma.cc/R8UW-P4JP] (providing recommendations on EU cybersecurity strategy). ENISA is the cyber security agency for the EU. *See About Enisa*, ENISA, https://www.enisa.europa.eu/about-enisa [https://perma.cc/MD9A-ZBLG].

[93] In addition, several European member states have recently updated their security requirements. In October 2016, France enacted the Digital Republic Bill which increased fines for failing to secure data, expanded data breach notification requirements, and allowed for increased investigations into companies' handling of data breaches.[400] In addition, in Europe collective legal proceedings can be brought against companies suspected of failing to secure their data.[401] These proceedings are similar to the U.S. class action suit. In Germany, recently enacted legislation permits the awarding of attorney's fees in such actions.[402] Because of this expanded potential liability, companies would be well-served to conduct frequent documented audits of their security practices. It is also important that data controllers ensure that their data processors are compliant as well.

11. Data Breach Notification Requirements

[94] Data breach notification requirements are not a new concept for American companies, but this is a new requirement under the GDPR. The 95 Directive did not require DPAs to be notified of a breach.[403] Article 33 reads:

> 1. 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

[400] *See* BENJAMIN WRIGHT, PREPARING FOR COMPLIANCE WITH THE GENERAL DATA PROTECTION REGULATION (GDPR) 1 (SANS Institute ed., 2017). This should be read in light of modifications made to French law since the application of the GDPR.

[401] *See id.* at 5.

[402] *See* Daniel Felz, *Germany's Christmas Present: Data-Protection Class Actions*, ALSTON & BIRD: PRIVACY & DATA SECURITY BLOG (Jan. 6, 2016), https://www.alstonprivacy.com/germanys-christmas-present-data-protection-class-actions/?cn-reloaded=1 [https://perma.cc/73ZC-BD7S].

[403] *See* GDPR, *supra* note 14, at recital 89.

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.

2. The *processor shall notify the controller* without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
    a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
    b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
    c. describe the likely consequences of the personal data breach;
    d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.[404]

As indicated earlier, many U.S. states have data breach notification statutes and companies have witnessed the severe ramifications to their peers for

[404] *Id.* at art. 33 (emphasis added).

failing to encrypt and secure PII.[405] Although Germany has had a data breach notification law for a number of years,[406] the GDPR will require all member states to require notification of data security breaches in certain conditions.[407] It is important to note that almost any breach will result in a conclusion that it resulted from the company's failure to properly secure its data.[408]

[95] Article 33 of the GDPR requires the company encountering a breach to notify the relevant supervisory authority not later than 72 hours after discovery, "unless the personal breach is unlikely to result in a risk to the rights and freedoms of natural persons."[409] Article 34 similarly requires notification to the natural persons who are the affected parties when it is likely to result in a high risk to their rights and freedoms, unless the data was encrypted or the company has taken measures to ensure that the data subjects' rights are not impacted.[410] In addition, processors must notify controllers of any breaches.[411]

[96] Despite the fact that some U.S. states have very short windows in which to notify users of a data breach, many U.S. companies take their time in determining the extent of a breach and its ramifications prior to sending

---

[405] *See, e.g.*, Maggie McGrath, *Target Profit Falls 46% on Credit Card Breach and The Hits Could Keep On Coming*, FORBES (Feb. 26, 2014, 9:21 AM), https://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profile-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/#3cc1b67f7326 [https://perma.cc/4XGS-R5TU].

[406] *See* Nikola Werry et. al., *Germany, in* THE PRIVACY, DATA PROTECTION, & CYBERSECURITY L. REV. 131 (Alan Charles Raul ed., 2017).

[407] *See* GDPR *supra* note 14, at art. 30.

[408] *See* WRIGHT, supra note 400, at 8.

[409] GDPR *supra* note 14, at art. 33.

[410] *See id.* at art. 34.

[411] *See id.* at art. 33(2).

out notifications to users.[412] This practice will not be sufficient under the GDPR. The 72-hour requirement will be especially problematic for companies wishing to keep the breach quiet until remediation can be accomplished, or a culprit found. Making the breach public will most likely alert the perpetrator who can then go silent.[413]

C. Steps for Compliance with the GDPR

[97] In order to comply with the GDPR, there are a number of steps which companies will need to take in order to technically comply. This section is not meant to serve as a complete explanation of all 99 articles of the GDPR, but rather some initial guidance to companies seeking to address compliance issues in advance of an investigation. Although not every company is required to have one,[414] the appointment of a DPO will go a long way to ensure that nothing is overlooked. As discussed in Section IV(B)(5) above, a DPO will be responsible for the record-keeping requirements,[415] which are significant. As a first step, companies must review the data currently maintained, consolidate all users' data records (at least by location), and determine if there is a lawful basis to keep the data and if proof of consent, if required, is documented.

[98] There are a number of lawful bases for which companies may collect data, such as a contractual obligation, but in many cases companies will

---

[412] *See Data Breach Charts*, BAKER HOSTETLER 23 (Jul. 2018), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf [https://perma.cc/S4BN-JLAF] (providing the guidelines for data breach notification in various states)*; see also* Hayley Tsukayama, *Why It Can Take So Long For Companies to Reveal Their Data Breaches*, WASH. POST, (Sept. 8, 2017) https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/why-it-can-take-so-long-for-companies-to-reveal-their-data-breaches/?utm_term=.d27d88036fe2 [https://perma.cc/K2UU-LCE2].

[413] *See* Tsukayama, *supra* note 412.

[414] *See* GDPR, *supra* note 14, at art. 27(2).

[415] *See* DLA Piper, *Key Changes*, *supra* note 281.

need to obtain consent from European users prior to collecting, processing, or storing their personal data and be able to provide documentation of such consent.[416] Companies will also need to inform the users of the purpose of such activities and the right to withdraw their consent.[417] In addition, the GDPR codifies the right to be forgotten and the right to data portability.[418] The GDPR will also delineate the responsibilities of data controllers and data processors.[419] Processors must provide "sufficient guarantees to implement appropriate technical and organizational measures" to comply with the GDPR.[420] This includes using appropriate measures to secure the data from possible breach.

[99] Going forward, privacy policies will need to be updated to fully disclose not only who the DPO and controller are, but also why information is being collected, and how users can exercise their rights. Privacy policies must be clear, concise and complete. Mechanisms should be developed that make it easy for users to exercise their rights and to consent to the collection of their data.

[100] Finally, training should be conducted for all employees. This is not solely an IT issue as failure of anyone in the organization to honor the rights of data subjects or comply with the requirements of the GDPR can result in significant fines. In addition to the issues of complying with the profiling requirement, the ability to document compliance and respond to data requests from users exercising their rights will be major issues. For everything discussed in Section IV(B), organizations will need to demonstrate how each requirement was accomplished (proof of impact assessments, privacy by design—meaning before introducing a new service

[416] See *GDPR Consent*, INTERSOFT CONSULTING, https://gdpr-info.eu/issues/consent/ [https://perma.cc/EYH2-KL8P].

[417] *See supra* Section IV(B)(4).

[418] *See* GDPR *supra* note 14, at arts. 17, 20.

[419] *See supra* Section IV(B)(1).

[420] *See* GDPR, supra note 14, at art. 28(1).

or product you must prepare a written report on how privacy was considered in the design, proof of lawful basis, consent records including consent for each separate use of the data). Individual data records will need to be easily accessible and available in machine-readable format.[421]

D. Cross-Border Data Transfers

[101] One issue particularly unique to the U.S. is the ability to transfer data from within the EU back to the U.S. Similar to the 95 Directive, the GDPR requires that before data can be transferred outside of the EU, the target country must provide adequate assurances of data protection.[422] Because the U.S. cannot provide such assurances due to its lack of similar privacy and data security laws, companies will need to either sign onto the Privacy Shield or use one of the other previously accepted methods of assuring adequate protection such as model contract clauses or binding corporate rules.[423]

1. Privacy Shield

[102] In 2016, the EU-U.S. Privacy Shield Framework was announced as a replacement to the Safe Harbor agreement that U.S. companies had previously operated under.[424] The Privacy Shield program, which is administered by the International Trade Administration (ITA) within the

[421] *See id.* at art. 20(1). As an aside, if an organization purchases marketing lists, it will now be required to obtain the consent record along with the list. It will no longer be sufficient to rely on the representation of the data broker. Finally, where once it was possible to add a prospect met at a trade show simply be virtue of a discussion and exchange of business cards, verifiable consent will need to be obtained prior to adding their personal data to a filing system (database).

[422] *See id.* at art. 44.

[423] *See generally id.* at arts. 44–50 (detailing under what conditions data may be transferred outside of the EU).

[424] *See* discussion *supra* Section II(A)(2) (on the declaration of the invalidity of the Safe Harbor in the Schrems case).

U.S. Department of Commerce, enables U.S.-based organizations to self-certify to the Privacy Shield, to benefit from the adequacy determinations, in order to allow the transfer of personal data from the European Union to the United States.[425] Companies become *certified* by agreeing to comply with seven primary data security principles, generally categorized as:

1. notice;
2. choice;
3. accountability for onward transfer;
4. security;
5. data integrity and purpose limitation;
6. access; and
7. recourse, enforcement, and liability.[426]

[103] One of the main differences between the Safe Harbor and the Privacy Shield is that under the Privacy Shield companies are required to ramp up their privacy policies to include more thorough notice requirements and better controls on further transfers of data. To become certified as compliant with the Privacy Shield, the company must first confirm eligibility, conduct a privacy audit, designate a privacy contact person in the company, post a privacy policy adopting the provisions of the Privacy Shield Principles, certify with the U.S. Department of Justice that it has agreed to the principles, and pay the certification fee of $250–$3,250.[427]

[104] Although U.S. companies are not required to join, once they commit, the provisions become enforceable under U.S. law.[428] All of the principles are designed to ensure adequate protection for personal

[425] *See Overview*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=OVERVIEW [https://perma.cc/9RKB-39ZW].

[426] *See id.*

[427] *See* DEP'T OF COM., HOW TO JOIN PRIVACY SHIELD: GUIDE TO SELF-CERTIFICATION (2016).

[428] *See id.*

information transfers from the European Union to the United States. The U.S. Department of Commerce, the FTC, and the DOT have enforcement authority.[429] As of November 1, 2018, 3948 companies were certified under the Privacy Shield.[430] Although it passed its first annual review in September 2017, it is likely that modifications will be necessary since the GDPR became effective on May 25, 2018.[431] There are still concerns that the Privacy Shield will need to be reevaluated. [432]

[429] *See Enforcement of Privacy Shield*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=Enforcement-of-Privacy-Shield [https://perma.cc/5PJD-CBDE].

[430] *See Privacy Shield List*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/list [https://perma.cc/V76C-DR76]

[431] *See* Press Release, *EU–U.S. Privacy Shield: First Reviews Shows it Works but Implementation Can be Improved*, EUR. COMMISSION (Oct. 18, 2017), http://europa.eu/rapid/press-release_IP-17-3966_en.htm [https://perma.cc/U8FZ-VY4M]. ("The report suggests a number of recommendations to ensure the continued successful functioning of the Privacy Shield: These include:

- More proactive and regular monitoring of companies' compliance with their Privacy Shield obligations by the U.S. Department of Commerce. The U.S. Department of Commerce should also conduct regular searches for companies making false claims about their participation in the Privacy Shield.
- More awareness-raising for EU individuals about how to exercise their rights under the Privacy Shield, notably on how to lodge complaints.
- Closer cooperation between privacy enforcers i.e. the U.S. Department of Commerce, the Federal Trade Commission, and the EU Data Protection Authorities (DPAs), notably to develop guidance for companies and enforcers.
- Enshrining the protection for non-Americans offered by Presidential Policy Directive 28 (PPD-28), as part of the ongoing debate in the U.S. on the reauthorisation and reform of Section 702 of the Foreign Intelligence Surveillance Act (FISA).
- To appoint as soon as possible a permanent Privacy Shield Ombudsperson, as well as ensuring the empty posts are filled on the Privacy and Civil Liberties Oversight Board (PCLOB)").

[432] *See* WEISS & ARCHICK, *supra* note 51, at 12.

2. Model Contract Clauses

[105] The European Commission permits alternatives to the Privacy Shield (or for destination countries other than the United States with inadequate privacy protections), the first major one being model contract clauses, the second being binding corporate rules (BCRs), and explicit consent agreements being a third. We will take them in that order but note that the first two of these—standard contractual clauses and BCRs—are conditioned on enforceable data subject rights and effective remedies for data subjects being available.[433]

[106] The European Commission has approved sets of standard contractual clauses that may be used between a company in the European Union exporting data, and another receiving company in a third country that does not have an adequate level of data protection.[434] The idea is that the contract clauses will bind the latter company legally to respect the essence of EU data protection law and provide data subjects with similar rights to those that they have under EU law.[435] In addition to referencing standard data protection clauses adopted by the Commission, the GDPR also refers to other adequate safeguards in the form of contract clauses.[436] These include "contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country…," subject to an authorization from the competent EU member state supervisory authority.[437]

[107] The European Commission has approved the following standard contractual clauses (or *model contracts*): EU controller to non-EU

[433] *See* GDPR, *supra* note 14, at art. 46(1).

[434] *See* Commission Decision No. 2001/497/EC, 2001 O.J. (L 181) ¶¶ [2], [5] [hereinafter 2001 Commission Decision].

[435] *See* GDPR, *supra* note 14, at art. 46(2).

[436] *See id.* at art. 46(3).

[437] *See id.*

controller (2001);[438] EU controller to non-EU controller (2004);[439] EU controller to a non-EU processor 2010)[440]

[108] It should be noted that, in light of the invalidation of the Safe Harbor agreement in the *Schrems* decision discussed above, and the recent challenge of standard contractual clauses in court in Ireland,[441] that there may be changes to the standard contractual clauses in the future.[442]

3. Binding Corporate Rules (BCRs)

[109] Article 47 of the GDPR expressly permits the use of binding corporate rules for the transfer of personal data to third countries or international organizations.[443] BCRs are "internal data protection and privacy rules set out by multinational companies to facilitate transfers of personal data," which set out the procedure for handling the processing of the data involving intra-company international transfers in a kind of self-certifying mechanism.[444] They may be approved by an individual EU member state DPA or may use a fast-track cooperation procedure for common opinions.[445] This instrument is provided for in the GDPR, as well,

[438] *See* 2001 Commission Decision, supra note 434, at 24–31.

[439] *See* Commission Decision No. 2004/915/EC, 2004 O.J. (L385) 74–83.

[440] *See* Commission Decision No. 2010/87/EU, 2010 O.J. (L 39) 5–18.

[441] *See generally* Data Prot. Comm'r v. Facebook Ireland Ltd., [2016] IR 4809 (H. Ct.) (Ir.) (analyzing the validity of standard contractual clauses).

[442] *See* LOTHAR DETERMANN, DETERMANN'S FIELD GUIDE TO DATA PRIVACY LAW: INTERNATIONAL CORPORATE COMPLIANCE 109 (3rd ed. 2017) (advising that companies should be prepared for changes and agree with their contracting partners to modify contracts when this becomes necessary).

[443] *See* GDPR, *supra* note 14, at art. 47.

[444] *See id.* at art. 4(20).

in order to allow cross-border transfers to non-adequate protection countries, such as the U.S.[446]

4. Explicit Consent Agreements

[110] In addition to model contract clauses and BCRs, explicit consent agreements are a third option in order to allow for cross-border data transfers under Article 49 of the GDPR. The data subject's consent to the cross-border transfer as signified by such instrument must be explicit and *informed*. In this context, the word *informed* means that prior to giving consent the individual must have been informed of the risks of transfers in the absence of an adequacy decision, model contract clauses, or a BCR, each of the latter two alternatives being considered an *adequate safeguard*.[447]

V. CONCLUSION

[111] The business model currently used by U.S. tech companies provides free access to services in exchange for a user's data.[448] This data can include information entered into a website or platform, searches, browsing history, likes and dislikes, as well as purchases. These companies are then able to monetize this data by selling it (or access to it) to advertisers.[449] Most

[445] *See Binding Corporate Rules*, EUR. COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en [https://perma.cc/473C-RYQH]

[446] *See* GDPR, *supra* note 14, at art. 46(2).

[447] *See id.* at art 49(1).

[448] *Cf.* Alex Johnson & Erik Ortiz, *Without Data-Targeted Ads, Facebook Would Look Like a Pay Service, Sandberg Says*, NBC NEWS (Apr. 5, 2018 9:06 PM), https://www.nbcnews.com/tech/social-media/users-would-have-pay-opt-out-all-facebook-ads-sheryl-n863151 [https://perma.cc/QPZ5-XY7A] (indicating that without targeting advertising, Facebook would need to charge its users).

[449] *See* G. S. Hans, *supra* note 5, at 164.

companies have not been able to successfully charge users to use their platforms,[450] thus it seems unlikely that U.S. tech companies will voluntarily change their business model because of the value of the data they can provide to advertisers. With respect to their users in the EU, rather than comply with the GDPR these companies may choose to move to an *agree or quit* model[451] or disallow those located in the EU from using their platform.[452] It was only with the Cambridge Analytica debacle that users in the U.S. began to understand that they were not merely trading data for access, but rather trading their privacy and security for services.[453]

[112] While many U.S. tech companies have informed the public that they will comply with GDPR,[454] the *data for service* model is unlikely to survive the review of the ECJ if actions are brought against these companies for violations. It is unlikely that this model would fall within *contractual obligation* or *legitimate interests* categories and thus consent must be obtained for each and every use, each and every future use, and for each

[450] *See Flexible Consumption: Transition to Pay-per-use Business Model*, DELOITTE, https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/solutions/pay-per-use-model-flexible-consumption-services.html# [https://perma.cc/8HHR-GLNE].

[451] *See* Frederik J. Zuiderveen Borgesius, et al., *Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation*, 3 EUR. DATA PROTECTION L. REV. 353, 354 (2017).

[452] *See* Hannah Kuchler, *US Small Businesses Drop EU Customers Over New Data Rule*, FIN. TIMES (May 24, 2018), https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04 [https://perma.cc/ZAE4-ZGCB].

[453] *See supra* Section II(C).

[454] *See* Matt Novak, *Facebook and Google Accused of Violating GDPR on First Day of the New European Privacy Law*, GIZMODO (May 25, 2018, 10:08 AM), https://gizmodo.com/facebook-and-google-accused-of-violating-gdpr-on-first-1826321323 [https://perma.cc/J4MJ-GGFP]. *See generally* Info. Commissioner's Off., Preparing for the General Data Protection Regulation (GDPR): 12 Steps to Take Now (Mar. 14, 2016), https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf [https://perma.cc/5PHZ-GCFN] (describing steps that companies can take now to comply with the GDPR).

sharing of the data. Users would be able to refuse any of these uses and sharing which would cripple the tech companies' ability to monetize the data.

[113] The maximum fines that can be imposed under the GDPR are significant. There are two levels of potential fines for noncompliance by companies.[455] Serious breaches can result in fines of up to 4% of annual global turnover or €20 Million (whichever is greater).[456] This could include lack of sufficient customer consent[457] to process data or violating the core of privacy by design concepts. Fines of up to 2% of global revenue may be assessed, for example, for failing to maintain proper records (Article 28)

[455] *See* Bernard Marr, *GDPR: The Biggest Data Breaches and the Shocking Fines (That Would Have Been)*, FORBES, (Jun. 11, 2018, 12:28 AM), https://www.forbes.com/sites/bernardmarr/2018/06/11/gdpr-the-biggest-data-breaches-and-the-shocking-fines-that-would-have-been/#220cf1fc6c10 [https://perma.cc/Z5BU-MKBJ].

[456] *Id*.

[457] *See* Shobhit Seth, *Google, Facebook Face $8.8B GDPR Suits on Day One*, INVESTOPEDIA (May 29, 2018, 2:51 PM), https://www.investopedia.com/news/google-facebook-face-88b-gdpr-suits-day-one/ [https://perma.cc/5FYN-SGGD]. As of the date of this article submission, DPAs in the EU have brought actions against both Facebook and Google.

and failing to provide data breach notifications on a timely basis.[458] These fines are applicable both to controllers and processors.[459]

[114] Many have noted that privacy laws in the U.S. need an overhaul.[460] The main statute regulating privacy in the U.S. is over 30 years old.[461] The Electronic Communications Privacy Act was written years before the widespread use of the Internet and long before social media.[462] Even the U.S. Department of Commerce has indicated that the lack of trust in Internet privacy in the U.S. is hampering economic activity.[463] Daniel Solove, a

[458] *See* GDPR, *supra* note 14, at art 83(4); *see also id.* at recital 75 (stating certain risks to the rights and freedoms of natural persons, specifically, "[w]here the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.")

[459] *See id.* at recital 79.

[460] *See* Christina Delgado, *Will Congress Finally Update a Data Privacy Law That's 31 Years Old?*, WASH. EXAMINER (Sept. 13, 2017, 1:01 PM), http://www.washingtonexaminer.com/will-congress-finally-update-a-data-privacy-law-thats-31-years-old/article/2634276 [https://perma.cc/SX5Q-PQ5S].

[461] *Id.*

[462] *See id.*

[463] *See* Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NAT'L TELECOMM. & INFO. ADMIN. (May 13,

privacy expert, repudiates the myth that the U.S. government is a leader in creating privacy and data protection laws pointing out that most of the federal laws were passed between 1970 and 1999.[464] While it is possible that the Cambridge Analytica fiasco will be the impetus the U.S. government needs to update its data protection and privacy laws, reluctance remains to move from the self-governance model to one of strict controls over data use using the GDPR as a model.

[115] The main reason for the differences in the laws and enforcement actions of the U.S. and EU with respect to U.S. tech companies is that the EU considers privacy to be an inalienable (or fundamental) right.[465] However, the U.S. Constitution does not even mention privacy.[466] The *Google Spain* case also elucidates the conflict between U.S. and the EU ideology with freedom of speech and the public right to know on the one hand, and the Europeans' right to privacy and to be forgotten on the other.[467]

2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities [https://perma.cc/EG62-SA7Q].

[464] *See* Daniel Solove, *The U.S. Congress Is Not the Leader in Privacy or Data Security Law*, TEACHPRIVACY (Apr. 9, 2017), https://www.teachprivacy.com/us-congress-is-not-leader-privacy-security-law/ [https://perma.cc/5UR8-LVBW].

[465] *See* Tony Wagner, *The Main Differences Between Internet Privacy in the US and the EU*, MARKETPLACE (Apr. 24, 2017, 4:22 PM), https://www.marketplace.org/2017/04/20/tech/make-me-smart-kai-and-molly/blog-main-differences-between-internet-privacy-us-and-eu [https://perma.cc/MVJ5-3DCY].

[466] *See* Warren & Brandeis, *supra* note 91, at 193 (detailing a common law right to privacy); *see also* James H. Barron, *Warren and Brandies,* The Right to Privacy, *4 HARV. L. REV 193 (1890): Demystifying a Landmark Citation*, 13 SUFFOLK U. L. REV. 875 (1979) (expanding on Warren and Brandeis' explanation of right to privacy); Ben Bratman, *Brandeis and Warren's* The Right to Privacy *and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623 (2002) (explaining the birth of the right to privacy finding its foundations in Warren and Brandeis' article).

[467] *See* discussion *supra* Section III(A)(1)(c); *see also* Jeffrey Rosen, Symposium, *The Right to be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88–91 (2012) ("In Europe, the intellectual roots of the right to be forgotten can be found in French law, which recognizes *le droit à l'oubli*—or the "right of oblivion"—a right that allows a convicted

While these conflicts are easily resolved in the EU where privacy is paramount, it is not so easy in the U.S.

[116] While the implementation of the GDPR will represent some issues for European companies to adapt to, they have already been operating under the strict privacy laws in effect since the 95 Directive and are in a much better position to comply. The interpretation of the GDPR will provide a test ground for this new business model and how it impacts the ability of companies to use and monetize consumer data. Although the GDPR represents a new paradigm for U.S. tech companies in terms of handling data, if it is successful, lessons learned could be adopted in the U.S. either voluntarily or by legal requirement.

[117] Although Mark Zuckerberg recently stated that changes to Facebook will provide additional protections to users worldwide, Facebook has also moved its data storage from the EU back to the U.S.[468] indicating that it may be preparing to challenge the applicability of the GDPR to its business practices. Given the European perception that these U.S. tech companies have had an unfair advantage due to lax American privacy laws and the shock of discovering the U.S. government's secret monitoring of data flowing out of the EU, it is likely that DPAs will watch carefully for failures to comply with the GDPR by these companies. There is an overriding sense of unfairness surrounding the ability of U.S. tech companies to monetize the data of those located in the EU where local tech companies cannot do the same due to the prohibitive restrictions of European data protection and privacy laws. Although the GDPR may not be the end of Facebook and Google, their business models and practices will have to be modified to take

criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction and incarceration. In America, by contrast, publication of someone's criminal history is protected by the First Amendment, leading Wikipedia to resist the efforts by two Germans convicted of murdering a famous actor to remove their criminal history from the actor's Wikipedia page.").

[468] *See* Alex Hern, *Facebook Moves 1.5bn Users Out of Reach of New European Privacy Law*, THE GUARDIAN (Apr. 19, 2018, 7:03 AM) https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law [https://perma.cc/PP6J-2AK8].

the new European legislation into account. It may, however, be fair to say that the new restrictions and fines may be an end to Facebook and Google as they currently operate, at least in the EU.